A light-weight secure protocol for small data dissemination in WSNs

Yan Wang, Daojing He (✉)

East China Normal University,
3663 N, Zhongshan Rd,Putuo District, Shanghai,China
boliangzai@foxmail.com,djhe@sei.ecnu.edu.cn

Abstract. This paper argues for a security scheme for security of data dissemination discovery and dissemination in WSNs, Wireless sensor networks. Our scheme is designed to be simple as well as has little impact on memory consumption and network traffic. The scheme is designed in light of issues derived from many different kinds of attacks.

Key words: Data discovery and dissemination, Security, Wireless sensor networks, Efficiency

1 Introduction

WSN consists of a lot of space-distributed sensors. To function a specific application,such as health-care, or obtain valuable information about physical world, Network manager needs every node work together though wireless channel.

Normally, WSNs collect data to a prime location named a base station. Base station could be your computer which allows network manager to store and analyse collected data later. On the other hand, each powerful sensor node has several parts, a circuit which is able to be interfaced with other devices, a battery for supplying electrical power, a radio transceiver.Actually, WSNs are usually deployed in hostile or remote area with many kinds of topology, such as ring, star.

Obviously, it is very important that a message should be protected from vicious attackers. And broadcast authentication is a very common security mechanism in WSNs, since broadcast authentication is able to provide message with confidentiality and authentication.

However , when message is been encrypted or authenticated , the cryptographic operations must be expensive for sensor node, since sensor node has limited resources. Hence, the attack can utilize this feature to launch Dos-attack. We provide two example to illustrate the above situation.

For example, in a smart-grid, the control center may broadcast adjustment parameter to every node in grid, adjusting the function of WSN, for example , tune the temperature surveillance to light perception.

All of the sensor networks is with limited resources. cryptographic operations is heavy on this network. Adversaries can send a large number of bogus messages and consume their resources.

when this situation, the attacker may have a lot of methods.

In an effort to make the message broadcast protocols in smart grids secure, Our contributions in this paper is organized as follows.

1)We firstly investigate the security problem in data discovery and dissemination protocol of WSNs and indicate the lack of authentication of disseminated data refers to a vulnerability. The energy in each sensor node is supplied by limited battery power or its energy harvesting capacity, thus it is significant to maintain energy to lengthen the operational lifetime of a sensor node.

2)second we balance the consumption of energy of every cryptographic techniques , select the most efficient methods or technique. We then design a secure, lightweight, robust method for smart grid. We may call it a extension of drip, our dissemination protocol for WSN.

3) we also implement our scheme practically using telosb. Experimental results demonstrate its high efficiency in practice.

In Section II, we review the related work and refine our work as well as possible. section III states the problem in WSNs we face, some assumption we have. section IV describes the security and efficiency performance of our protocol. Section VI describes the implementation and experimental performance in real sensor node. Finally, Section VII concludes this paper.

2 related work

Data dissemination is within the scope of broadcast authentication. There is a lot of challenges on providing security in our smart grid. The primary one is the limited computing, communication and storage capabilities of receivers. A message authentication code (MAC) is usually an authentication tag derived by applying an authentication scheme and a secret key to a message. MAC is an efficient symmetric cryptographic primitive for two-party authentication, but it is not suitable for broadcast communication. Because the sender and its receivers share the same secret key, any one of the receivers can impersonate the sender and forge vicious messages to other receivers. Which means asymmetric mechanisms is more suitable for broadcast authentication. More exactly, the sender signs each packet individually using digital signature technique and each receiver verifies the signature before processing the packet. The signature is vulnerable to Dos attacks. That is, the adversary may flood a large number of illegal packets to receivers to exhaust their limited resources and render them less capable of serving legitimate users. To provide authentication, some researchers proposed TESLA and its various extensions to authenticate broadcast packets in a network [7][9]. It employs symmetric cryptography primitives with delayed key disclosure to achieve the effect of asymmetric mechanism, more specifically, the key used to authenticate current message is to be disclosed in next message. However these methods requires time synchronization in the whole network, which leads to more complicated measures to secure synchronization. In addition, the receivers cannot authenticate packets immediately, but have to wait until the respective keys are disclosed, resulting in excessive verification latency and a requirement

to store unauthenticated packets. What's more, this protocol has some disadvantage, such as, non-repudiation, one-way key chain that has a predefined-length, short duration. Dos attack [2] and non-repudiation. Some other researchers proposed one-time signature schemes. Unfortunately, such schemes suffer from large key size and a limited number of keys is available.Biba

Recently, since packet contains signature means a big consumption in delivery, some signature amortization protocol, EMSS, has been proposed.. With EMSS [5], periodic signature pakcets are sent after every N data packets. Thus, all the packets that arrive before their signature packet have to wait to be verified. In another protocol [**?**] , First packet contains a signature of next packet, signature is signed on hash of next packet, and recusively, current packet contains hash of next packets.

3 Review on Message Dissemination

Drip is one of the most popular message dissemination protocols in sensor networks. In Drip, each message is represented as 3-tuple(key, seqno, data), where key uniquely identifies the variable to be updated, data denotes the disseminated data item(e.g., parameter, command or query), and seqno indicates if the data item is old or new(the larger the seqno, the newer the data). In the Drip implementation, key and seqno are 2 bytes and 4 bytes long respectively. Drip disseminates each data item with a separate instance of Trickle algorithm. Once new data are injected to a network, it will soon be disseminated by Trickle quickly [6]. In the rest of this paper, unless otherwise specified, we assume that Drip is used as the message dissemination protocol.

4 PROBLEM DEFINITION

4.1 Network Model

We consider a broadcast group involving one sender (S) and a group of receivers (R i). Each message is delivered from S to each R through lossy and insecure PLC network, as illustrated in Fig. 4. The intermediate receivers in the network only forward the packets and do not provide any security measure (such as integrity and authenticity checks). These receivers may also be malicious and drop or modify Ss packets or even inject fake packets. We consider a class of applications where 1) each generated message is unknown to S until it is ready to send; 2) S (resp. R) signs (resp. verifies) the message once it appears; 3) the sending rate at S is dynamic. The data flow of the broadcast authentication protocol is shown in Fig. 5.

4.2 requirement

In addition to the asymmetric mechanism that is needed for broadcast authentication, an efficient and secure broadcast authentication scheme for smart grids should still satisfy the following requirements:

1) Individual authentication: The receiver should verify the received packets individually without depending onother packets; otherwise, the failure to verify a packet prevents the verification of subsequent packets.

2) Robust to packet loss: The smart grid communication environment is not reliable; therefore, the scheme should be able to cope with the loss of packets during trans- mission.

3) Short authentication latency: Many PLC applications are real time applications, e.g. sending the control informa- tion to the customers. To authenticate real time data, the maximum number of additional packets that need to be received before a packet can be authenticated should be small.

4) Low computation cost: Receivers have limited compu- tation power. Thus, they should only perform a small number of operations to verify a packet.

5) Receiver compromise tolerance: The protocol should be resilient to receiver compromise attack no matter how many receivers have been compromised, as long as the subset of non-compromised receivers can still form a connected graph with the trusted source.

6) Low communication overhead: Because a PLC network often is restricted in bandwidth, the number of bytes per packet used for authentication should be small.

7) DoS attacks resistance: The functions of the PLC net- work should not be disrupted by DoS attacks.

8) Freshness: A receiver should be able to differentiate whether an incoming message is the newest version.

9) Scalability: The protocol should be efficient even for large-scale smart grids with thousands of receivers.

10) Low storage requirement: Since the storage space of receivers is limited, some data for authentication like key material and signatures stored in memory cannot be too large.

11) Data Confidentiality: In some critical applications, the data items from the sender are strictly private and confidential. They should be encrypted to protect the data privacy from eavesdroppers. If the broadcast data items are chosen from a small finite set, the encryption should produce ciphertext that does not give information to an intruder on which of these messages was sent. Ideally, we would like a scheme that recovers from any loss of packets, has no authentication latency, can individually authenticate packets and ensure data confidentiality, has neg- ligible overhead, and has a low computation cost. In practice, such a perfect scheme is difficult to achieve, and a compromise needs to be found between these requirements.

4.3 Assumptions

Our protocol makes the following assumptions.

The sender cannot be compromised, and is trusted. In Drip, the sender is the origin of all legitimate message updates. The sender has unlimited computational power compared with receiver.

The receiver can perform a limited number of asymmetric cryptographic operations such as signature verification in TinyECC [15], but they cannot afford to perform many such operations due to their energy limitations.

5 THE PROPOSED PROTOCOL

Before giving the detailed description of the proposed protocol, we first provide an overview of our protocol.

5.1 Overview of Our Protocol

Compared with the traditional approaches, Compared with the traditional approaches, elliptic curve cryptography (ECC) is a better approach to public-key cryp- tography in terms of key size, computational efficiency, and communication efficiency. However, this signature is vul- nerable to DoS attacks.

References

1. Smith, T.F., Waterman, M.S.: Identification of Common Molecular Subsequences. J. Mol. Biol. 147, 195–197 (1981)
2. Grover K, Lim A.: A survey of broadcast authentication schemes for wireless networks[J]. Ad Hoc Networks, 2015, 24: 288-316.
3. Perrig A.: The BiBa one-time signature and broadcast authentication protocol[C]//Proceedings of the 8th ACM conference on Computer and Communications Security. ACM, 2001: 28-37.
4. He D, Chan S C, Guizani M.: Small data dissemination for wireless sensor networks: The security aspect[J]. Wireless Communications, IEEE, 2014, 21(3): 110-116.
5. Perrig A, Canetti R, Tygar J D, et al.: Efficient authentication and signing of multicast streams over lossy channels[C]//Security and Privacy, 2000. IEEE Symposium on. IEEE, 2000: 56-73.
6. Patel N, Culler D, Shenker S.: Trickle: A self regulating algorithm for code propagation and maintenance in wireless sensor networks[M]. Computer Science Division, University of California, 2003.
7. May, P., Ehrlich, H.C., Steinke, T.: ZIB Structure Prediction Pipeline: Composing a Complex Biological Workflow through Web Services. In: Nagel, W.E., Walter, W.V., Lehner, W. (eds.) Euro-Par 2006. LNCS, vol. 4128, pp. 1148–1158. Springer, Heidelberg (2006)
8. Foster, I., Kesselman, C.: The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann, San Francisco (1999)

9. Czajkowski, K., Fitzgerald, S., Foster, I., Kesselman, C.: Grid Information Services for Distributed Resource Sharing. In: 10th IEEE International Symposium on High Performance Distributed Computing, pp. 181–184. IEEE Press, New York (2001)
10. Foster, I., Kesselman, C., Nick, J., Tuecke, S.: The Physiology of the Grid: an Open Grid Services Architecture for Distributed Systems Integration. Technical report, Global Grid Forum (2002)
11. National Center for Biotechnology Information, http://www.ncbi.nlm.nih.gov