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

[1] 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

My work starts at a survey of broadcast, I read a lot of related work them. 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.

2.1 Existing Work on Broadcast Authentication

2.2 Review on Message Dissemination

3 problem definition

3.1 Network Model

We consider a broadcast group involving one sender and a group of receivers, every message should be passed through insecure wireless channel. If there are cryptographic techniques on sensor node, we then have to perform lightweight scheme.

3.2 detailed requirement

In addition to asymmetric mechanism that is needed for broadcast authentication, an efficient and secure broadcast authentication scheme for smart grids should still satisfy the following requirement: 1) Individual authentication: The receiver should verify the received packets individually without depending on other packet, otherwise, the failure to verify a packet prevent 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 transmission.

3) short authentication latency

4) Low computation

5) receiver compromise tolerance

6) Low power comsumption

7) Freshness

8) scalability: the protocol should be able to be inclusive of new node joing the network.

9) Freshness

10) Low storage requirement

11) Data confidentiality

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 negligible overhead, and has a low computation cost. In practice, such a perfect scheme is difficult to achieve, and a compromise needs to be found to reach a better achievement.

3.3 Assumption

Our protocol believe in the following assumptions .

The sender cannot be compromised.

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 cite, but they cannot afford to perform too many such operations due to their limited computing capabilities.

4 the proposed protocol

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

4.1 Overview of Our protocol

Compared to other asymmetric signature approaches, elliptic curve cryptographic is a well-behaved approach to public-key cryptography in terms of key size, computational efficiency, and communication efficiency. However, this signature is vulnerable to Dos attacks. To resist such Dos attacks, some researchers employed the Message Specific Puzzle (MSP) and included the puzzle solution in an message packet. In our protocol, we think over the Cipher Puzzle (CP) to integrate confidentiality and Dos-resistance. We choose Message specific puzzles as our solution to counter Dos attack. Actually, Both of them are difficult for adversary to construct a legitimate packet. The computational effort of theses two puzzles for the sender are similar but the difficulty for an adversary to construct.

We know that merits of the cp is that you cannot launch brute attack, since the first l bytes of hash result is different for each message being broadcasted.

5 security and efficiency analysis

6 implementation and performance

7 conclusion

References

1. Smith, T.F., Waterman, M.S.: Identification of Common Molecular Subsequences. J. Mol. Biol. 147, 195–197 (1981)
2. 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)
3. Foster, I., Kesselman, C.: The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann, San Francisco (1999)
4. 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)
5. 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)
6. National Center for Biotechnology Information, http://www.ncbi.nlm.nih.gov