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

5 security and efficiency analysis

6 implementation and performance

7 conclusion

8 references

9 Checking the PDF File

Kindly assure that the Contact Publication Chair is given the name and email address of the contact author for your paper. The Contact Publication Chair uses these details to compile a list for our production department at SPS in India. Once the files have been worked upon, SPS sends a copy of the final pdf of each paper to its contact author. The contact author is asked to check through the final pdf to make sure that no errors have crept in during the transfer or preparation of the files. This should not be seen as an opportunity to update or copyedit the papers, which is not possible due to time constraints. Only errors introduced during the preparation of the files will be corrected.

This round of checking takes place about two weeks after the files have been sent to the Editorial by the Contact Publication Chair, i.e., roughly seven weeks before the start of the conference for conference proceedings, or seven weeks before the volume leaves the printer's, for post-proceedings. If SPS does not receive a reply from a particular contact author, within the timeframe given, then it is presumed that the author has found no errors in the paper. The tight publication schedule of LNICST does not allow SPS to send reminders or search for alternative email addresses on the Internet.

In some cases, it is the Contact Publication Chair that checks all the final pdfs. In such cases, the authors are not involved in the checking phase.

9.1 Additional Information Required by the Publication Chair

If you have more than one surname, please make sure that the Publication Chair knows how you are to be listed in the author index.

9.2 Copyright Forms

LNICST has integrated its copyright form into the paper submission system which means that you must agree with transferring the copyrights of your paper while uploading your camera ready version to the submission system. The author who uploads the paper should be the author who has the authority to agree with the terms of the copyright agreement on behalf of all the authors. After confirming the agreement the author will receive an e-mail with the filled document which is confirmed by both the author and ICST.

10 Paper Preparation

Springer provides you with a complete integrated LaTeX document class (`SVMultln.cls`) for multi-author books and the associated class option file (`svlnicst.clo`) to get the layout for the LNICST series. Papers not complying with the LNICST style will be reformatted. This can lead to an increase in the overall number of pages. We would therefore urge you not to squash your paper.

Please always cancel any superfluous definitions that are not actually used in your text. If you do not, these may conflict with the definitions of the macro package, causing changes in the structure of the text and leading to numerous mistakes in the proofs.

If you wonder what LaTeX is and where it can be obtained, see the "*LaTeX project site*" (`http://www.latex-project.org`) and especially the webpage "*How to get it*" (`http://www.latex-project.org/ftp.html`) respectively.

When you use LaTeX together with our document class file, `SVMultln.cls` and the documentclass option `lnicst`, your text is typeset automatically in Computer Modern Roman (CM) fonts. Please do *not* change the preset fonts. If you have to use fonts other than the preset fonts, kindly submit these with your files.

Please use the commands `\label` and `\ref` for cross-references and the commands `\bibitem` and `\cite` for references to the bibliography, to enable us to create hyperlinks at these places.

For preparing your figures electronically and integrating them into your source file we recommend using the standard LaTeX `graphics` or `graphicx` package. These provide the `\includegraphics` command. In general, please refrain from using the `\special` command.

Remember to submit any further style files and fonts you have used together with your source files.

Headings. Headings should be capitalized (i.e., nouns, verbs, and all other words except articles, prepositions, and conjunctions should be set with an initial capital) and should, with the exception of the title, be aligned to the left. Words joined by a hyphen are subject to a special rule. If the first word can stand alone, the second word should be capitalized.

Here are some examples of headings: "Criteria to Disprove Context-Freeness of Collage Language", "On Correcting the Intrusion of Tracing Non-deterministic Programs by Software", "A User-Friendly and Extendable Data Distribution System", "Multi-flip Networks: Parallelizing GenSAT", "Self-determinations of Man".

Lemmas, Propositions, and Theorems. The numbers accorded to lemmas, propositions, and theorems, etc. should appear in consecutive order, starting with Lemma 1, and not, for example, with Lemma 11.

10.1 Figures

For LaTeX users, we recommend using the *graphics* or *graphicx* package and the `\includegraphics` command.

Please check that the lines in line drawings are not interrupted and are of a constant width. Grids and details within the figures must be clearly legible and may not be written one on top of the other. Line drawings should have a resolution of at least 800 dpi (preferably 1200 dpi). The lettering in figures should have a height of 2 mm (10-point type). Figures should be numbered and should have a caption which should always be positioned *under* the figures, in contrast to the caption belonging to a table, which should always appear *above* the table; this is simply achieved as matter of sequence in your source.

Please center the figures or your tabular material by using the `\centering` declaration. Short captions are centered by default between the margins and typeset in 9-point type (Fig. 1 shows an example). The distance between text and figure is preset to be about 8 mm, the distance between figure and caption about 6 mm.

To ensure that the reproduction of your illustrations is of a reasonable quality, we advise against the use of shading. The contrast should be as pronounced as possible.

If screenshots are necessary, please make sure that you are happy with the print quality before you send the files.

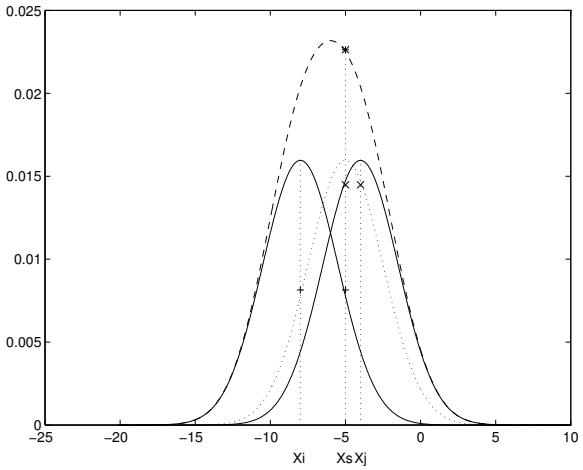

Fig. 1. One kernel at x_s (*dotted kernel*) or two kernels at x_i and x_j (*left and right*) lead to the same summed estimate at x_s. This shows a figure consisting of different types of lines. Elements of the figure described in the caption should be set in italics, in parentheses, as shown in this sample caption.

Please define figures (and tables) as floating objects. Please avoid using optional location parameters like "`[h]`" for "here".

Remark 1. In the printed volumes, illustrations are generally black and white (halftones), and only in exceptional cases, and if the author is prepared to cover the extra cost for color reproduction, are colored pictures accepted. Colored pictures are welcome in the electronic version free of charge. If you send colored figures that are to be printed in black and white, please make sure that they really are legible in black and white. Some colors as well as the contrast of converted colors show up very poorly when printed in black and white.

10.2 Formulas

Displayed equations or formulas are centered and set on a separate line (with an extra line or halfline space above and below). Displayed expressions should be numbered for reference. The numbers should be consecutive within each section or within the contribution, with numbers enclosed in parentheses and set on the right margin – which is the default if you use the *equation* environment, e.g.

$$\psi(u) = \int_o^T \left[\frac{1}{2} \left(\Lambda_o^{-1} u, u \right) + N^*(-u) \right] dt \, . \tag{1}$$

Please punctuate a displayed equation in the same way as ordinary text but with a small space before the end punctuation.

10.3 Footnotes

The superscript numeral used to refer to a footnote appears in the text either directly after the word to be discussed or – in relation to a phrase or a sentence – following the punctuation sign (comma, semicolon, or period). Footnotes should appear at the bottom of the normal text area, with a line of about 2 cm set immediately above them.[1]

10.4 Program Code

Program listings or program commands in the text are normally set in typewriter font, e.g., CMTT10 or Courier.

Example of a Computer Program

```
program Inflation (Output)
  {Assuming annual inflation rates of 7%, 8%, and 10%,...
   years};
   const
     MaxYears = 10;
   var
     Year: 0..MaxYears;
```

[1] The footnote numeral is set flush left and the text follows with the usual word spacing.

```
    Factor1, Factor2, Factor3: Real;
  begin
    Year := 0;
    Factor1 := 1.0; Factor2 := 1.0; Factor3 := 1.0;
    WriteLn('Year  7% 8% 10%'); WriteLn;
    repeat
      Year := Year + 1;
      Factor1 := Factor1 * 1.07;
      Factor2 := Factor2 * 1.08;
      Factor3 := Factor3 * 1.10;
      WriteLn(Year:5,Factor1:7:3,Factor2:7:3,Factor3:7:3)
    until Year = MaxYears
end.
```

(Example from Jensen K., Wirth N. (1991) Pascal user manual and report. Springer, New York)

10.5 Citations

For citations in the text please use square brackets and consecutive numbers: [1], [2], [3], [4] – provided automatically by LaTeX's `\cite` ... `\bibitem` mechanism.

10.6 Page Numbering and Running Heads

There is no need to include page numbers. If your paper title is too long to serve as a running head, it will be shortened. Your suggestion as to how to shorten it would be most welcome.

11 LNICST Online

The online version of the volume will be available in LNICST Online. Members of institutes subscribing to the Lecture Notes in Business Information Processing series have access to all the pdfs of all the online publications. Non-subscribers can only read as far as the abstracts. If they try to go beyond this point, they are automatically asked, whether they would like to order the pdf, and are given instructions as to how to do so.

12 BibTeX Entries

The correct BibTeX entries for the Lecture Notes in Computer Science volumes can be found at the following Website shortly after the publication of the book:
`http://www.informatik.uni-trier.de/~ley/db/journals/lncs.html`

Acknowledgments. The heading should be treated as a subsubsection heading and should not be assigned a number.

13 Advances in References

In order to permit cross referencing within LNCS/LNICST-Online, and eventually between different publishers and their online databases, LNCS/LNICST will be standardizing the format of the references. This feature will increase the visibility of publications and facilitate academic research considerably. Please base your references on the examples below. References that don't adhere to this style will be reformatted by Springer. You should therefore check your references thoroughly when you receive the final pdf of your paper. The reference section must be complete. You may not omit references. Instructions as to where to find a fuller version of the references are not permissible.

The following section shows a sample LNCS/LNICST reference list with 6 entries for journal articles [1], a LNCS/LNICST chapter [2], a book [3], proceedings without editors [4] and [5], as well as an URL [6]. Please note that proceedings published in LNICST are not cited with their full titles, but with their acronyms!

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

Appendix: Springer-Author Discount

LNICST authors are entitled to a 33.3% discount off all Springer publications. Before placing an order, the author should send an email to `SDC.bookorder@springer.com`, giving full details of his or her Springer publication, to obtain a so-called token. This token is a number, which must be entered when placing an order via the Internet, in order to obtain the discount.

14 Checklist of Items to be Sent to Publication Chairs

Here is a checklist of everything the publication chair requires from you:

☐ The final LaTeX source files

☐ A final PDF file