A Verifiable Secure protocol in a Secure System

plusminus

plusminus M1915001

plusminus

plusminus

Abstract

Distributed querying and monitoring systems have been widely studied in recent years. These systems aim to maintain data sources, such as data set or log files, and allow users to query over those data sources. When the data sources are highly related and users only care some statistic results, like the sum or the average, it is consumed to transmit all data sources via the network. To minimize the network consumption, in-network aggregation technique is proposed. However, this technique is subject to some known attacks, such as the injection attack and the pollution attack. Prior works only considered the settings that data sources are trusted while the network is not. We study the way to relax the limitation and guarantee the aggregate queries robust to malicious or faulty data sources (also called polluted data sources).

Acknowledgements

plusminus plusminus plusminus plusminus

Contents

List of Figures

List of Tables

List of Algorithms

Chapter 1 Introduction

Security in wireless sensor networks (WSNs) has become a popular research field in recent years, and node identification is considered as one of the most important issues in this field [1]. In WSNs, the mechanism to create and manage node identities is usually naive and is not well protected. Thus many attack techniques, such as Sybil attacks and replication attacks, are used to exploit this vulnerability.

Since the node identities are easy to create and change, a reliable node identification mechanism is needed in sensor networks. Currently several authentication and certification methods have been proposed to ensure the node identification. However, these approaches use cryptographic techniques, and thus inevitably increase computing overhead of sensor nodes. This chapter introduces a simple but effective method to identify a node only by measuring its clock skew.

Recently, Chen et al. revealed the possibility to fingerprint every computer in general networks by their clock skews. Murdoch's research also used clock skew as a main method to detect the identities behind the Tor network. However, there are few studies evaluating the characteristics of clock skew in WSNs [2]. In this research, we use the Flooding Time Synchronization Protocol (FTSP) to measure the time information of each mote, and successfully observe that every sensor mote does have constant and unique clock skew [3–6]. An algorithm to group and identify clock skews of large amount of motes is proposed, and its applications like Sybil attack detection are also discussed in Table 1.1.

Generally, there are two steps to measure the clock skew between two devices. The first step is to collect the timestamp from the sender via a certain protocol. After collecting enough timestamp, the receiver will apply a clock skew estimation algorithm (such as linear regression, linear programming or piecewise minimum), to calculate the clock skew in the second step. Due to different network environments, we need to use different protocols and estimation algorithms to calculate clock skews. Since we will apply clock skew device identification to different networks, such as wireless sensor networks and cloud environment, more detailed procedures will be discussed in each chapter.

Table 1.1: The relation of aggregation overhead between different techniques

	Space usage of root aggregator	Communication overhead	Query requirement
Traditional warehouse	n	$O(n)$	$O(n)$
AM-FM sketch technique	$\log a$	$O(\log n)$	$O(a \log n)$
“prototypical PHI query”	$\log a$	$O(\log n)$	$O(\log n)$

Chapter 2 Preliminaries

With the rapid growth in integrated circuit, digital signal processing, and other emerging technologies, people nowadays can easily purchase electronic devices, such as personal computers, laptops, cellular phones, and tablets. By utilizing these devices, people can communicate with each other through wireless communication and increase work performance. However, any malicious user may misuse these devices and launch serious attack to make illegal profit, such as identity stealing or password cracking on a bank account. Therefore, it is essential to develop robust methods to solve the identity problems. With the rapid growth in integrated circuit, digital signal processing, and other emerging technologies, people nowadays can easily purchase electronic devices, such as personal computers, laptops, cellular phones, and tablets. By utilizing these devices, people can communicate with each other through wireless communication and increase work performance. However, any malicious user may misuse these devices and launch serious attack to make illegal profit, such as identity stealing or password cracking on a bank account. Therefore, it is essential to develop robust methods to solve the identity problems. With the rapid growth in integrated circuit, digital signal processing, and other emerging technologies, people nowadays can easily purchase electronic devices, such as personal computers, laptops, cellular phones, and tablets. By utilizing these devices, people can communicate with each other through wireless communication and increase work performance. However, any malicious user may misuse these devices and launch serious attack to make illegal profit, such as identity stealing or password cracking on a bank account. Therefore, it is essential to develop robust methods to solve the identity problems, as shown in 2.1.

Figure 2.1: The diagram of “prototypical PHI query”

Chapter 3 Conclusions

With the rapid growth in integrated circuit, digital signal processing, and other emerging technologies, people nowadays can easily purchase electronic devices, such as personal computers, laptops, cellular phones, and tablets. By utilizing these devices, people can communicate with each other through wireless communication and increase work performance. However, any malicious user may misuse these devices and launch serious attack to make illegal profit, such as identity stealing or password cracking on a bank account. Therefore, it is essential to develop robust methods to solve the identity problems.

3.1 Future Work

With the rapid growth in integrated circuit, digital signal processing, and other emerging technologies, people nowadays can easily purchase electronic devices, such as personal computers, laptops, cellular phones, and tablets. By utilizing these devices, people can communicate with each other through wireless communication and increase work performance. However, any malicious user may misuse these devices and launch serious attack to make illegal profit, such as identity stealing or password cracking on a bank account. Therefore, it is essential to develop robust methods to solve the identity problems.

References

[1] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "Tag: A tiny aggregation service for ad-hoc sensor networks," in *Proceedings of the 5th Symposium on Operating Systems Design and Implementation (OSDI)*, vol. 36, (Boston, Massachusetts, USA), pp. 131–146, ACM, Dec 2002.

[2] M. N. Garofalakis, J. M. Hellerstein, and P. Maniatis, "Proof sketches: Verifiable in-network aggregation," in *Proceedings of IEEE 23rd International Conference on Data Engineering (ICDE)*, (Istanbul, Turkey), pp. 996–1005, Apr 2007.

[3] Y. Kotidis, V. Vassalos, A. Deligiannakis, V. Stoumpos, and A. Delis, "Robust management of outliers in sensor network aggregate queries," in *Proceedings of the 6th ACM International Workshop on Data Engineering for Wireless and Mobile Access (MobiDE)*, (Beijing, China), pp. 17–24, ACM, Jun 2007.

[4] S. Subramaniam, T. Palpanas, D. Papadopoulos, V. Kalogeraki, and D. Gunopulos, "Online outlier detection in sensor data using non-parametric models," in *Proceedings of the 32nd International Conference on Very Large Data Bases (VLDB)*, (Seoul, Korea), pp. 187–198, VLDB Endowment, Sep 2006.

[5] B. Sheng, Q. Li, W. Mao, and W. Jin, "Outlier detection in sensor networks," in *Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, (Montreal, Quebec, Canada), pp. 219–228, ACM, Sep 2007.

[6] D. Wagner, "Resilient aggregation in sensor networks," in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, (Washington DC, USA), pp. 78–87, ACM, Oct 2004.