A Secure Model for Detecting Origin Forgery and Packet Drop Attacks in Wireless Network

P. Sharmila
Research Scholar
Department of Computer Science & Engineering
Science Shrimati Indira Gandhi College, Trichy

P. Ananthi
Assistant Professor
Department of Computer and Application
Science Shrimati Indira Gandhi College, Trichy

Abstract

Since data are originated and processed by multiple agents in wireless sensor networks, data provenance plays an important role for assuring data trustworthiness. Large-scale sensor networks are deployed in numerous application domains, and the data they collect are used in decision making for critical infrastructures. Data are streamed from multiple sources through intermediate processing nodes that aggregate information. A malicious adversary may introduce additional nodes in the network or compromise existing ones. Therefore, assuring high data trustworthiness is crucial for correct decision-making. Data provenance represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. In this paper, a novel lightweight scheme to securely transmit provenance for sensor data is proposed. The proposed technique relies on in-packet Bloom filters to encode provenance. An efficient mechanism for provenance verification and reconstruction at the base station is introduced. In addition, extended the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. Experimental results prove the effectiveness and efficiency of the lightweight secure provenance scheme in detecting packet forgery and loss attacks.

Keywords: Provenance, security, sensor networks

I. INTRODUCTION

The Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. In a Wireless sensor networks sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data towards to a sink, which could be a gateway, base station or storage node. Securing the Wireless Sensor Networks need to make the network support all security properties: confidentiality, integrity, authenticity and availability. A sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are supposed to forward. We expect sensor networks to consist of hundreds or thousands of sensor nodes . Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attack. The networks may be dispersed over a large area, further exposing them to attackers who capture and reprogram individual sensor nodes. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the network, the adversary can then mount a variety of attack

II. LITERATURE SURVEY

A. A. Ramachandran, K. Bhandankar, M. Tariq, and N. Feamster, "Packets with Provenance," Technical Report GT-CS-08-02, Georgia Tech, 2008.

This paper presents the design, analysis, user-space implementation, and evaluation of Pedigree, which consists of two components: a trusted tagger that resides on hosts and tags packets with information about their provenance (i.e., identity and history of potential input from hosts and resources for the process that generated them), and an arbiter, which decides what to do with the traffic that carries certain tags. Pedigree allows operators to write traffic classification policies with expressive semantics that reflect properties of the actual process that generated the traffic.

1) Drawback

This scheme assumes a trusted environment which is not realistic in sensor networks

All rights reserved by *www.ijste.org*

B. *W. Zhou, M. Sherr, T. Tao, X. Li, B. Loo, and Y. Mao, "Efficient Querying and Maintenance of Network Provenance at InternetScale," Proc. ACM SIGMOD Int'l Conf. Management of Data, pp. 615-626, 2010*

This paper presents the design and implementation of ExSPAN, a generic and extensible framework that achieves efficient network provenance in a distributed environment. ExSPAN uses declarative networking in which network protocols can be modeled as continuous queries over distributed streams and specified concisely in a declarative query language.

The ExSPAN prototype is developed using RapidNet, a declarative networking platform based on the emerging ns-3 toolkit. Experiments over a simulated network and an actual deployment in a testbed environment demonstrate that this system supports a wide range of distributed provenance computations efficiently, resulting in significant reductions in bandwidth costs compared to traditional approaches.

Drawback

This system also does not address security concerns and is specific to some network use cases.

C. *W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. Loo, and M. Sherr, "Secure NetworkProvenance,"Proc.ACMSOSP,pp.295-310,2011.*

This paper introduces secure network provenance (SNP), a novel technique that enables networked systems to explain to their operators why they are in a certain state – e.g., why a suspicious routing table entry is present on a certain router, or where a given cache entry originated. SNP provides network forensics capabilities by permitting operators to track down faulty or misbehaving nodes, and to assess the damage such nodes may have caused to the rest of the system. SNP is designed for adversarial settings and is robust to manipulation; its tamper-evident properties ensure that operators can detect when compromised nodes lie or falsely implicate correct nodes.

Drawback

This system is not optimized for the resource constrained sensor networks.

D. *S. Chong, C. Skalka, and J.A. Vaughan, "Self-Identifying Sensor Data," Proc. Ninth ACM/IEEE Int'l Conf. Information Processing in Sensor Networks (IPSN), pp. 82-93, 2010.*

This technique is similar to traditional watermarking but is intended for application to unstructured datasets. This approach is potentially imperceptible given sufficient margins of error in datasets, and is robust to a number of benign but likely transformations including truncation, rounding, bit-flipping, sampling, and reordering. It provides algorithms for both one-bit and blind mark checking. These algorithms are probabilistic in nature and are characterized by a combinatorial analysis.

Drawback

It is not intended as a security mechanism, hence, does not deal with malicious attacks
Practical issues like scalability, data degradation, etc. have not been well addressed

III. EXISTING SYSTEM

- Recent research highlighted the key contribution of provenance in systems where the use of untrustworthy data may lead to catastrophic failures (e.g., SCADA systems). Although provenance modeling, collection, and querying have been studied extensively for workflows and curated databases, provenance in sensor networks has not been properly addressed.
- Pedigree captures provenance for network packets in the form of per packet tags that store a history of all nodes and processes that manipulated the packet.
- Hasan et al. propose a chain model of provenance and ensure integrity and confidentiality through encryption, checksum and incremental chained signature mechanism.
- Chong et al. embed the provenance of data source within the data set.

A. *Drawbacks of existing system*

- Traditional provenance security solutions use intensively cryptography and digital signatures, and they employ append-based data structures to store provenance, leading to prohibitive costs.
- Employs separate transmission channels for data and provenance

B. *Proposed System*

- We investigate the problem of secure and efficient provenance transmission and processing for sensor networks, and we use provenance to detect packet loss attacks staged by malicious sensor nodes.
- Our goal is to design a provenance encoding and decoding mechanism that satisfies such security and performance needs. We propose a provenance encoding strategy whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the provenance information. We also devise an extension of the provenance encoding scheme that allows the BS to detect if a packet drop attack was staged by a malicious node.Specific contributions are,

All rights reserved by *www.ijste.org*

- An arithmetic coding based, distributed, and lossless provenance encoding mechanism for WSN. Our scheme also supports data aggregation.
- An efficient technique for provenance decoding and verification at the base station.
- A secure mechanism for assigning and sharing the occurrence probabilities of a particular node that are used in arithmetic coding. Our mechanism ensures confidentiality so that no malicious node can decode the provenance information of other nodes.
- A secure packet sequence number generation mechanism

C. *Advantages of Proposed System*

- We use only fast message authentication code (MAC) schemes and Bloom filters, which are fixed-size data structures that compactly represent provenance. Bloom filters make efficient usage of bandwidth, and they yield low error rates in practice.
- We formulate the problem of secure provenance transmission in sensor networks, and identify the challenges specific to this context.
- We propose an in-packet Bloom filter (iBF) provenance-encoding scheme.
- We design efficient techniques for provenance decoding and verification at the base station.
- We extend the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.

We perform a detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism.

IV. ALGORITHM IMPLEMENTATION

A. *Gradient Descent Algorithm*

Gradient descent algorithm is popular and handles for very large-scale optimization problems. It is also known as steepest gradient mathematical method. Gradient descent algorithm in jamming attacks on encoding and decoding localization. It sequence of solutions that approach a traffic control without files or data destroyed. The basic idea of Gradient Descent is to use a loop to adjust the model based on the error it observes between its predicted output and the actual output. The adjustment node is pointing to a direction where the error is decreasing in the steepest sense (hence the term "gradient").
It defined so this approach can be applicable in a wide range of machine learning scenarios.

- The Model
- The loss function
- The learning rate

Gradient Descent is very popular method because of the following reasons...

- Intuitive and easy to understand.
- Easy to run incrementally with additional data
- On the other hand, the greedy approach in Gradient Descent can be trapped in local optimum. This can be mitigated by choosing a convex LOSS function (which has a single node), or multiple starting points can be picked randomly generated.

V. IMPLEMENTATION

The goal is to design a provenance encoding and decoding mechanism which satisfies security and performance needs. It proposes a provenance encoding strategy in that each node on the path of a data packet securely embeds provenance information within a Bloom filter (BF) should be transmitted along with the data. While receiving the packet the Base Station extracts and verifies the provenance information. The extension of the provenance encoding scheme allows the BS to detect packet drop

We formulate the problem of secure provenance transmission in sensor networks.

- The implementation of an in-packet Bloom filter provenance encoding Scheme.
- To design efficient techniques for provenance decoding and verification at the base station.
- To design mechanism that detects *packet drop attacks* staged by malicious forwarding sensor nodes.
- To perform a detailed security analysis and performance Evaluation.
  - The fast message authentication code (MAC) schemes and Bloom filters are fixed-size data structures that efficiently represent provenance.
  - Bloom filters make efficient usage of bandwidth, and they yield low error rates
  - Claim for Confidentiality: - iBF is computationally infeasible to an attacker to gain data about the sensor nodes included in the provenance.
  - Claim For Integrity: - An attacker, acting as single user or colluding with others in the group cannot successfully add or legitimate nodes to the data generated by the compromised/already attack happened nodes.

All rights reserved by *www.ijste.org*

- An attacker or a set of cooperative attackers cannot selectively add or remove nodes from the provenance of data generated by legitimate nodes.
- A malicious aggregator cannot selectively drop a child node from the provenance.
- Claim For Freshness:- Provenance replay attacks are detected by the provenance scheme.

VI. CONCLUSION AND FUTURE WORK

This survey addressed the problem of how securely transmitting provenance for sensor networks. Based on Bloom filters this paper proposed a light-weight provenance encoding and decoding scheme. The scheme ensures confidentiality, integrity and freshness of provenance. Also this scheme extended to incorporate data-provenance joining, and to include packet sequence information that supports detection of packet loss attacks. The proposed scheme is considered as effective, light-weight and scalable. This survey plan implements a real system prototype of secure provenance scheme, and to increase the accuracy of packet loss detection, especially in the case of multiple uninterrupted malicious sensor nodes.

We addressed the problem of securely transmitting provenance for sensor networks, and proposed a light-weight provenance encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance. We extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable. In future work, we plan to implement a real system prototype of our secure provenance scheme, and to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

REFERENCES

[1] H. Lim, Y. Moon, and E. Bertino, "Provenance-Based Trustworthiness Assessment in Sensor Networks," Proc. Seventh Int'l WorkshopData Management for Sensor Networks, pp. 2-7, 2010.
[2] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A Virtual Data System for Representing, Querying, and Automating Data
[3] Derivation," Proc. Conf. Scientific and Statistical Database Management,pp. 37-46, 2002.
[4] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-Aware Storage systems," Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006. Y. Simmhan, B. Plale, and D. Gannon, "A Survey of Data Provenancein E-Science," ACMSIGMODRecord, vol. 34, pp. 31-36, 2005.
[5] R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance," Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14, 2009.
[6] S. Madden, J. Franklin, J. Hellerstein, and W. Hong, "TAG: A TinyAggregation Service for Ad-Hoc Sensor Networks," ACM SIGOPS Operating Systems Rev., vol. 36, no. SI, pp. 131-146, Dec. 2002.
[7] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An Efficient Clustering Based Heuristic for Data Gathering and Aggregation in Sensor Networks," Proc. Wireless Comm. and Networking Conf., pp. 19481953, 2003.
[8] S. Sultana, E. Bertino, and M. Shehab, "A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks," Proc. Int'l Conf. Distributed Computing Systems (ICDCS) Workshops, pp. 332-338, 2011.
[9] L. Fan, P. Cao, J. Almeida, and A.Z. Broder, "Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol," IEEE/ACM Trans. Networking, vol. 8, no. 3, pp. 281-293, June 2000.
[10] A. Kirsch and M. Mitzenmacher, "Distance-Sensitive BloomFilters," Proc. Workshop Algorithm Eng. and Experiments, pp. 41-50, 2006.

All rights reserved by *www.ijste.org*