Scientific Journal of Impact Factor (SJIF): 3.134

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 1, January -2016

Provenance Forgery and Packet Drop Attacks Detection in Wireless Networks

Suraj Ramdas Bhadale[1], Prof. Shrikant Nagure [2]

[1,2]*Department Of Computer, Rmd Sinhgad School Of Engineering*

Abstract — *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, we propose a novel lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on in packet Bloom filters to encode provenance. We introduce efficient mechanisms for provenance verification and reconstruction at the base station. In addition, we extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. We evaluate the proposed technique both analytically and empirically, and the results prove the effectiveness and efficiency of the lightweight secure provenance scheme in detecting packet forgery and loss attacks.*

Keywords*-Data provenance, Wireless Sensor Network, Bloom Filtering, Encryption, Decryption.*

I. INTRODUCTION

Sensor networks are becoming increasingly popular in numerous application domains, such as cyber physical infrastructure systems, environmental monitoring, power grids, etc. Data are produced at a large number of sensor node sources and processed in-network at intermediate hops on their way to a base station that performs decision-making. The diversity of data sources creates the need to assure the trustworthiness of data, such that only trustworthy information is considered in the decision process. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data. 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 for critical infrastructure. Although provenance modeling, collection, and querying have been investigated extensively for workflows and curated databases, provenance in sensor networks has not been properly addressed. In this paper, we investigate the problem of secure and efficient provenance transmission and processing for sensor networks.

In a multi-hop sensor network, data provenance allows the base station to trace the source and forwarding path of an individual data packet since its generation. Provenance must be recorded for each data packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of the sensor nodes. Therefore, it is necessary to devise a light-weight provenance solution which does not introduce significant overhead. Furthermore, sensors often operate in an untrusted environment, where they may be subject to attacks. Hence, it is necessary to address security requirements such as confidentiality, integrity and freshness of provenance. 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, which is transmitted along with the data. Upon receiving the data, the base station extracts and verifies the provenance.

II. LITERATURE REVIEW

Sr. No.	Paper Name	Author	Published Year	Description
1	A Lightweight Secure Scheme forDetecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks.	Salmin Sultana,Gabriel Ghinita, Elisa Bertino, Fellow, and Mohamed Shehab	2015	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. proposed a novel lightweight scheme to securely transmit provenance for sensor data.
2	Secure Data Aggregation in	Sankardas Roy, Mauro Conti,	2013	The paper discuss the security issues of in-network aggregation algorithms to compute aggregates such as

	Wireless Sensor Networks	Sanjeev Setia, and Sushil Jajodia		predicate Count and Sum also discussed how a compromised node can corrupt the aggregate estimate of the base station, keeping our focus on the ring-based hierarchical aggregation algorithms. To address this problem, presented a lightweight verification algorithm which would enable the base station (BS) to verify whether the computed aggregate was valid.
3	In-packet Bloom filters: Design and networking applications	Christian E. Rothenberg, Carlos A. B. M., Maur´ıcio F. Magalhaesa, F´abio L. V., A. Wiesmaierc	2011	This paper explores an exciting front in the Bloom filter research space, namely the special category of small Bloom filters carried in packet headers. Using iBFs is a promising approach for networking application designers choosing to move application state to the packets themselves. At the expense of some false positives, fixed-size iBFs are amenable to hardware and present a way for new networking applications.
4	Provenance based Trustworthiness Assessment in Sensor Networks	Hyo Sang Lim, Yang Sae Moon, South Korea Elisa Bertino	2010	Proposed a systematic method for assessing the trustworthiness of data items. This approach uses the data provenance as well as their values in computing trust scores, that is, quantitative measures of trustworthiness. To obtain trust scores, proposed a cyclic framework which well reflects the inter-dependency property: the trust score of the data affects the trust score of the network nodes that created and manipulated the data, and vice-versa.

III. SURVEY OF PROPOSED SYSTEM

Goals:

1. **Confidentiality:** An adversary cannot gain any knowledge about data provenance by analyzing the contents of a packet. Only authorized parties (e.g., the BS) can process and check the integrity of provenance.
2. **Integrity:** An adversary, acting alone or colluding with others, cannot add or remove non-colluding nodes from the provenance of benign data (i.e. data generated by benign nodes) without being detected.
3. **Freshness:** An adversary cannot replay captured data and provenance without being detected by the BS.

Objectives:

1. We formulate the problem of secure provenance transmission in sensor networks, and identify the challenges specific to this context.
2. We propose an in-packet BF provenance-encoding scheme.
3. We design efficient techniques for provenance decoding and verification at the base station.
4. We perform a detailed security analysis and performance evaluation of the proposed technique.

IV. PROPOSED ALGORITHM

4.1 Description of functions

1. sender:

The user will perform following functions:
-send_data ()
-check_trustworthiness ()

2. Provenance:
-encoding ()
-decodig()
-collection()
-verfication ()

3. in-packet filtering:
-bloom_filter ()
-alert_msg()

4.2 Mathematical Model

Let W be the whole system which consists:

W= {IP, PRO, OP}
IP is the input of system.
IP= {BS, G, N, L, K, H, d, ID, V, E, S, BF}.
Where,

1. Let BS is the Base Station which collects data from network.

2. Let G is the graph , G(N,L)
   Where, N is the set of nodes.

   N = {ni|, 1 ≤ i ≤ |N|} is the set of nodes,
   And L is the set of links, containing an element li,j for each pair of nodes ni and nj that are communicating directly with each other.

3. K is set of symmetric cryptographic key

4. H is a set of hash functions

   H = {h1, h2, ..., hk} .

5. E is edge set consists of directed edges that connect sensor nodes.

6. d is the set of data packets,

Let G is acyclic graph G(V,E) where each vertex v ∈ V is attributed to a specific node HOST(v) = n and represents the provenance record (i.e. nodeID) for that node.

Each vertex in the provenance graph is uniquely identified by a vertex ID (VID) which is generated by the host node using cryptographic hash functions.

Procedure:
Let S is a set of items
S = {s1, s2, ..., sn}
We use an array of m bits with k independent hash functions h1, h2, ..., hk.
The output of each hash function hi maps an item s uniformly to the range [0, m-1], i.e., an index in a m-bit array.
Let BF is the Bloom Filer, can be represented as {b0, . . . , bm−1}.
Initially all m bits are set to 0.
To insert an element s ∈ S into a BF, s is hashed with all the k hash functions producing the values hi(s) (1 ≤ i ≤ k).
The bits corresponding to these values are then set to 1 in the bit array.
To query the membership of an item s` within S, the bits at indices hi(s`) (1 ≤ i ≤ k) are checked. If any of them is 0, then certainly s` not within S. Otherwise, if all of the bits are set to 1, s`∈ S with high probability.

There exists a possibility of error which arises due to hashing collision that makes the elements in S collectively causing indices hi(s`) being set to 1 even if s` not within S. This is called a false positive.

V. SYSTEM ARCHITECTURE

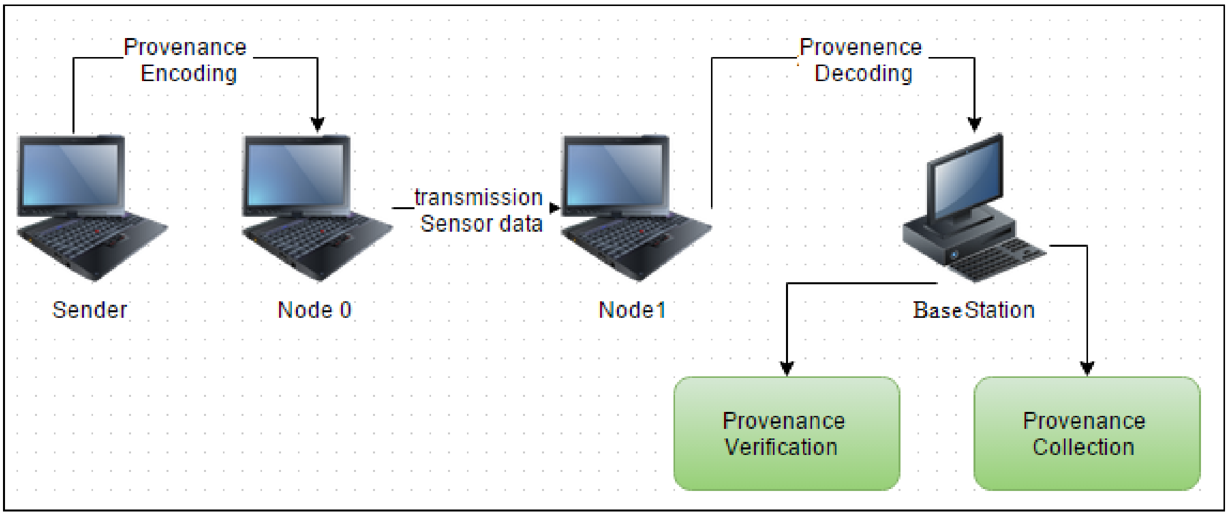

Fig 5.1 System Architecture

Sensor networks are becoming increasingly popular in numerous application domains, such as cyberphysical infrastructure systems, environmental monitoring, power grids, etc. Data are produced at a large number of sensor node sources and processed in-network at intermediate hops on their way to a base station that performs decision-making. The diversity of data sources creates the need to assure the trustworthiness of data, such that only trustworthy information is considered in the decision process. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data.

VI . CONCLUSION AND FUTURE WORK

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.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFERENCES

1. H. Lim, Y. Moon, and E. Bertino, “Provenance-based trustworthiness assessment in sensor networks,” in *Proc. of Data Management for Sensor Networks*, 2010, pp. 2–7.
2. S. Sultana, E. Bertino, and M. Shehab, “A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks,” in *Proc. of ICDCS Workshops*, 2011, pp. 332–338.
3. L. Fan, P. Cao, J. Almeida, and A. Z. Broder, “Summary cache: a scalable wide-area web cache sharing protocol,” *IEEE/ACM Trans. Netw.*, vol. 8, no. 3, pp. 281–293, Jun. 2000.
4. Kirsch and M. Mitzenmacher, “Distance-sensitive bloom filters,” in *Proc. of the Workshop on Algorithm Engineering and Experiments*, 2006, pp. 41–50.
5. Rothenberg, C. Macapuna, M. Magalhaes, F. Verdi, and A. Wiesmaier, “In-packet bloom filters: Design and networking applications,” *Computer Networks*, vol. 55, no. 6, pp. 1364 –1378, 2011.
6. S. Roy, M. Conti, S. Setia, and S. Jajodia, “Secure data aggregation in wireless sensor networks,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1040–1052, 2012.
7. I. Foster, J. Vockler, M. Wilde, and Y. Zhao, “Chimera: A virtual data system for representing, querying, and automating data derivation,” in *Proc. of the Conf. on Scientific and Statistical Database Management*, 2002, pp. 37–46.
8. K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, “Provenance-aware storage systems,” in *Proc. of the USENIX Annual Technical Conf.*, 2006, pp. 4–4.
9. Y. Simmhan, B. Plale, and D. Gannon, “A survey of data provenance in e-science,” *SIGMOD Record*, vol. 34, pp. 31–36, 2005.
10. R. Hasan, R. Sion, and M. Winslett, “The case of the fake picasso: Preventing history forgery with secure provenance,” in *Proc. Of FAST*, 2009, pp. 1–14.
11. S. Madden, J. Franklin, J. Hellerstein, and W. Hong, “TAG: a tiny aggregation service for ad-hoc sensor networks,” *SIGOPS Operating Systems Review*, no. SI, Dec. 2002.
12. K. Dasgupta, K. Kalpakis, and P. Namjoshi, “An efficient clustering based heuristic for data gathering and aggregation in sensor networks,” in *Proc. of Wireless Communications and Networking Conference*, 2003, pp. 1948–1953.
13. A. Kirsch and M. Mitzenmacher, “Distance-sensitive bloom filters,” in *Proc. of the Workshop on Algorithm Engineering and Experiments*, 2006, pp. 41–50.
14. C. Rothenberg, C. Macapuna, M. Magalhaes, F. Verdi, and A. Wiesmaier, “In-packet bloom filters: Design and networking applications,” *Computer Networks*, vol. 55, no. 6, pp. 1364 – 1378, 2011.
15. S. Roy, M. Conti, S. Setia, and S. Jajodia, “Secure data aggregation in wireless sensor networks,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1040–1052, 2012.

AUTHORS

Suraj Ramdas Bhadale,Pursuing M.E In Computer Science At Rmd Sinhgad School Of Engineering, 111/1, Pune-Mumbai Bypass Highway, Warje, Pune, Maharashtra 411058 Tal:- Haveli, Dist.:- Pune- 411058