IJCTA, 9(14) 2016, pp. 6349-6353
© International Science Press

Secure Provenance Scheme for Wireless Sensor Networks

G. S. P. Krishna*[*] and A. Meena Priyadarshini[**]**

ABSTRACT

Large-scale sensor systems are helpful in various application areas, and the information they gather are utilized as a part of decision making for basic foundations. Information is surged from numerous sources through intermediate nodes that aggregate the data. A malicious opponent may enter with the data by introducing additional nodes in the network. Information provenance is a key component in assessing the reliability of sensor information. Provenance administration for sensor systems presents a few testing prerequisites, for example, low vitality and data transfer capacity utilization, efficient capacity, and secure transmission. A novel lightweight plan is proposed to transmit safe provenance for sensor information. The proposed system depends on in-packet Bloom filters to encode provenance. Efficient mechanism for provenance verification and reconstructing at the base station is introduced. The proposed technique is evaluated both logically and experimentally, and the outcomes demonstrate the effectiveness and efficiency of the lightweight secure provenance plan in recognizing packet assembling and unwanted attacks.

Index terms: Provenance, Bloom Filter, Security

I. INTRODUCTION

WSN are turning out to be progressively well-known in various application spaces, for example, cyber-physical infrastructure systems, environmental monitoring, power grids, and so forth. Information is delivered at countless hub sources and prepared in-network at intermediate hops on their way to a base station that performs choice making. The assorted qualities of information sources make the need to guarantee the dependability of information, such that just reliable data is considered in the choice procedure. Data provenance is a viable strategy to survey information dependability since it compresses the historical backdrop of proprietorship and the activities performed on the information. According to the recent research the commitment of provenance in systems where the utilization of untrustworthy information might prompt unfortunate failures (e.g., SCADA systems). In spite of the fact that provenance displaying, collection, and questioning have been examined widely for workflows and curated databases, provenance in sensor systems has not been legitimately addressed. In this paper, we explore the issue of secure and efficient provenance transmission and handling for sensor systems.

In a multi-hop sensor system, data provenance permits the base station to follow the source and sending way of an individual data packet since its generation. Provenance must be recorded for every data packet, yet vital difficulties emerge because of the tight storage, vitality and transmission capacity limitations of the sensor nodes. Consequently, it is essential to devise a light-weight provenance arrangement which does not bring significant overhead. Moreover, sensors regularly work in an untrusted situation, where they might be liable to attacks. Thus, it is important to address security necessities, for example, confidentiality, uprightness and freshness of provenance. We will likely outline a provenance encoding and decoding

[*] Student, M.Tech Computer Science and Engineering, Department of Computer Science and Engineering, SRM University, Kattankulathur-603203, Chennai, India, *E-mail: Phanikrishna.ganti@gmail.com*

[**] Assistant Professor (O.G), Department of Computer Science and Engineering, SRM University, Kattankulathur-603203, Chennai, India

component that satisfies such security and execution needs. We propose a provenance encoding procedure whereby every node on the way of a data packet safely implants provenance data inside of a *Bloom ûlter* (BF) that is transmitted alongside the data. After receiving the data, the base station extracts and veriûes the provenance.

Rather than existing exploration that utilizes separate transmission channels for data and provenance, we just require a solitary channel for both. Such a methodology is more reasonable for WSN. Moreover, conventional provenance security arrangements utilize seriously cryptography and digital signatures, and they use append based data structures to store provenance, prompting restrictive expenses. Conversely, we utilize Bloom ûlters (BF), which are ûxed-size data structures that minimally represent provenance. BFs makes efûcient use of transmission capacity, and regardless of the possibility that they just give probabilistic decoding ensured, they yield low blunder rates in practice.

Our speciûc commitments are:

- We define the issue of secure provenance transmission in sensor organizes, and recognize the difficulties speciûc to this context.
- We propose an in-packet BF provenance-encoding.
- We outline efûcient strategies for provenance decoding and veriûcation at the base station.
- We perform detailed security examination and performance evaluation of the proposed system.

2. SYSTEM MODEL

In this section, we explain the network, data and provenance models used. We also introduce the security requirements. Finally, we provide a brief explanation on Bloom ûlters, their fundamental properties, and operations.

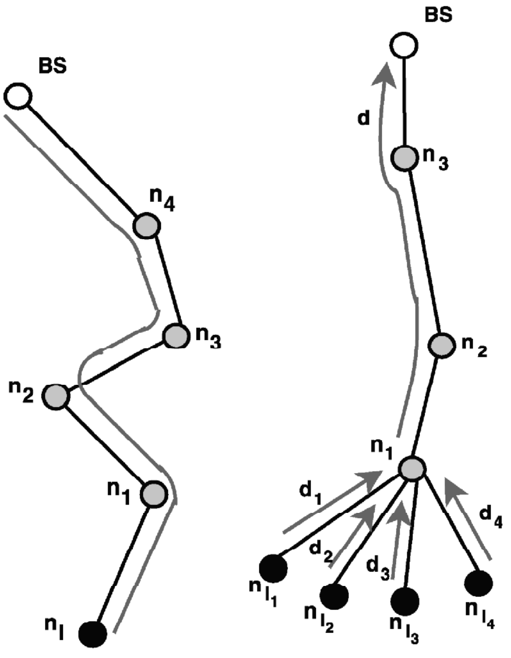
2.1. Network Model

We consider a multihop remote sensor system, comprising of various sensor nodes and a base station (BS) that gathers information from the system. The system is displayed as a Graph C (N, L), where $N = \{n_i|, 1 \leq i \; |N|\}$ is the arrangement of nodes, and L is the arrangement of connections, containing a component, $l_{i,j}$ for every pair of nodes n_i and n_j that are corresponding specifically with each other. Sensor nodes are stationary after sending, yet routing paths might change over the long haul, e.g., because of node failure. Every node reports its neighboring node data to the BS after sending. The BS defines every node a one of a kind identifier *nodelD* And a symmetric cryptographic key K_i. Also, an arrangement of hash capacities $H = \{h_1, h_2,..., hk\}$ are shown to nodes to use amid provenance enclosed.

2.2. Data Model

We accept a various round procedure of data accumulation. Every sensor creates data intermittently, and individual values are routed and accumulated towards the BS utilizing any current hierarchical schemes (tree-based). A data path of D hops is spoken to as <n_l; n_1; n_2;...; n_d >, where n_l is a leaf node speaking to the data source, and node n_i is i hops far from n_l. Each non-leaf node in the path totals the received data and provenance with its own privately created data and provenance. Each data packet has unique sequence number and a data value with provenance attached to the packet.

Each data packet contains 1) a unique SID, 2) a data value, and 3) provenance. The sequence numbers are attached to the packet data initializer, and all nodes use the same sequence number for given round. The sequence number integrity is ensured through MACs



(a) (b)

Figure 1: Provenance graphs for a sensor network

2.3. Provenance Model

This model describes how provenance is attached to the data packets by using encoding and decoding schemes. As data packets are transmitted through nodes, provenance encoding is done at each node which is involved in data processing.

Considering a data packet d, provenance is displayed as DAG A (V, E) where each vertex $v \in V$ is credited to specific node HOST (v) = n which represents provenance record for that node. Each vertex has unique VID, generated using Hash functions by host node. The Edge set S consists of directed edges connecting sensor nodes.

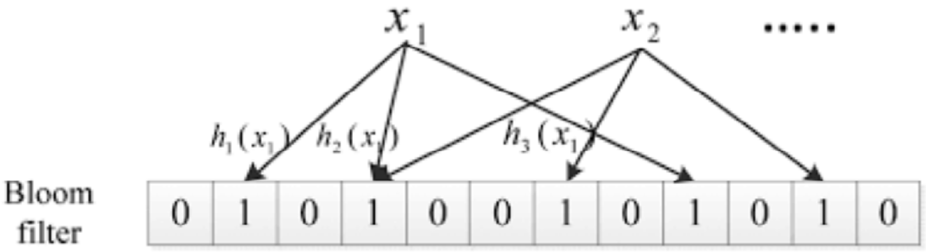
Figure 1 show two provenance examples where in figure 1(a) the leaf node n_1 creates a data packet d, and each intermediate node totals the sensory data with d then forwards it to Base Station. On the other hand figure, 1(b) aggregates the data d_1 to d_4 from n_1 to n_4 and the passes d to BS.

2.4. Security Objectives

Assuming base station is trusted, but any other self-assertive node may be malicious. An adversary can spy and perform traffic analysis anywhere on path and may deploy malicious nodes. In addition, adversary may compromise the nodes and overwrite their memory. The primary concern is that an attacker may misrepresent the data provenance where data packet with no provenance records is highly suspicious. The objectives are:

- Confidentiality**:** Processing and checking the integrity of the data packet can be done by the authorized parties like BS, where an adversary cannot get any information about the provenance by analyzing the packet.
- Integrity: An adversary alone or conspiring with other nodes cannot tamper the non-conspiring nodes from the provenance of gentle data, without being detected.

Bloom Filter (BF). A bloom filter is a space- efficient data structure for probabilistic data representation



X = {x_1, x_2,..., x_n} using an array of *m* bits with *k* independent hash functions h_1, h_2,..., h_k. The output of each hash function h_i maps an item *s* uniformly to the range [0, m-1] and is elucidated as an index indicating to a bit in a *m*-bit array. Hence, the BF can be represented as {b_0,..., b_{m-1}}. At first, each of the *m* bits is set to 0.

The cumulative nature of BF construction inherently supports the aggregation of BFs of the same kind, by performing bitwise-OR between the bitmaps.

3. SECURE PROVENANCE SCHEMES

Encoding of a data packet and decoding the provenance are tendered through different mechanisms, In-Packet Bloom filter (*iBF)* is the main aspect maintaining the provenance data. Each packet has unique data value and sequence number, and *iBF* holds the provenance.

- *Provenance Encoding*: Provenance encoding is done at each node through data packets which have unique sequence number on which they are distinguished, and a secret key is attached to the data packet of host node. BF is created along with the data packet by the source node and all the values are initialized as 0's. Every intermediate node aggregates the provenance along with their provenance record. When the packet reaches BS, *iBF* contains provenance records of all the nodes.
- *Provenance Decoding:* When the packet reaches BS, it starts provenance verification assuming that the path is known to BS and checks iBF whether the correct path has been followed.

The below Architecture design illustrates how the data is being transferred, and nodes are interconnected in the network through a gateway to the Base Station.

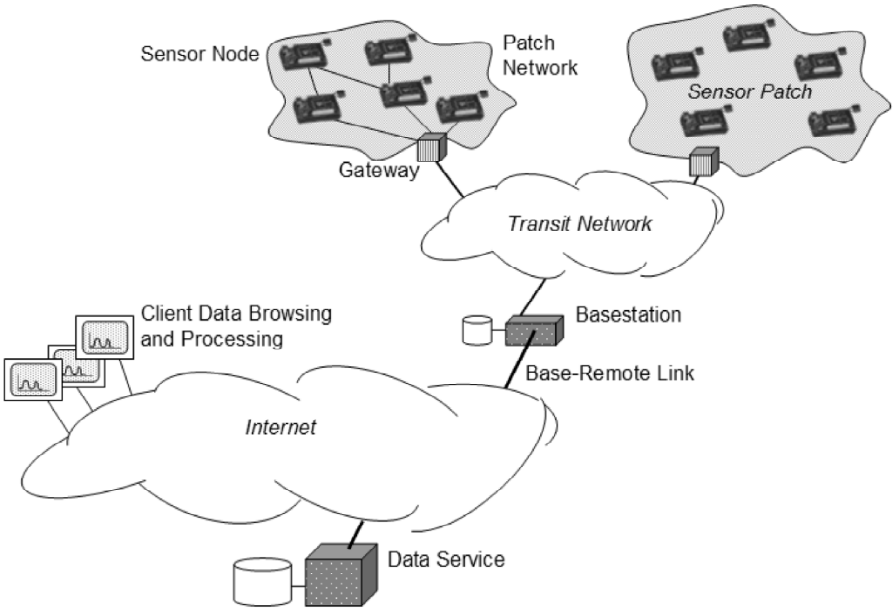


Figure 2: Architecture diagram

The procedure that extricates the overall flow of control for data transmission is shown in the Fig. 2. The diagram explains the step by step procedure for transmission of a packet and how the provenance verification process is done can be demonstrated.

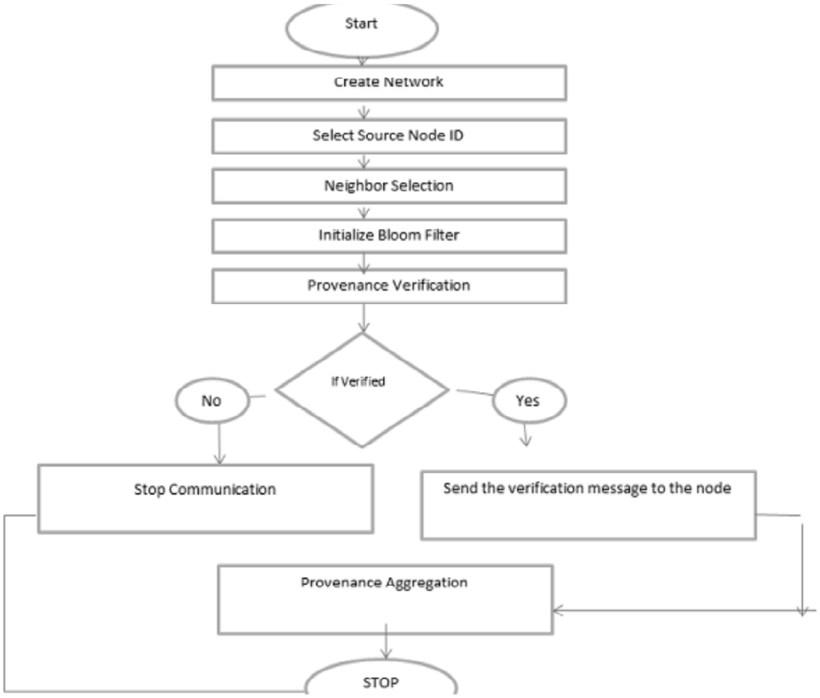


Figure 3: Data-Flow Diagram

4. IMPLEMENTATION

Provenance collection and Provenance verification are the major techniques which rely on the secure transmission of data. Key generation and using a hash index for provenance encoded packets so as to maintain the cryptographic measures for reliable and secure transmission of a data packet.

Traditional cryptographic algorithm RSA is used cipher text and binding the provenance. Provenance encoding and decoding have a different approach in executing.

5. CONCLUSION

The problem of secure transmission of provenance for sensor networks, a light-weight provenance encoding and decoding scheme based on Bloom filters has been introduced which maintains confidentiality, integrity and freshness of provenance. Unique packet sequence number helps in detect packet loss attacks. In future work, we plan to implement a framework of our secure provenance scheme, to improve the accuracy of packet loss detection.

REFERENCES

[1] W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. Loo, and M. Sherr, “Secure network provenance,” in Proc. of ACM SOSP, 2011, pp. 295–310.

[2] Y. Simmhan, B. Plale, and D. Gannon, “A survey of data provenance in e-science,” SIGMOD Record, vol. 34, pp. 31–36, 2005.

[3] 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,

[4] S. Sultana, M. Shehab, and E. Bertino, “Secure provenance transmission for streaming data,” *IEEE TKDE*, 2012.

[5] S. Sultana, M. Shehab, and E. Bertino, “Secure provenance transmission for streaming data,” *IEEE TKDE*, 2012.