A Model for Identifying Source of Packet Drops and Forgery Attacks in WSN

Ambika
PG Scholar, CSE, Lingraj Appa Engineering College Bidar
Email: moreambika20@gmail.com

Nirupama S
Assistant Professor, CSE, Lingraj Appa Engineering College Bidar
Email: nirupama.sheelwant@gmail.com

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. This survey proposes a new lightweight scheme in order to securely transmit provenance with sensor data. The proposed in-packet Bloom filters technique is used to encode provenance with the sensor data. This mechanism initially performs provenance at the base station, then performs reconstruction of the data at the base station. In addition to this, the provenance scheme functionality is used to detect packet drop attacks organized by malicious data forwarding nodes.

Keywords: Bloom Filters, Packet Drop, Provenance Decoding, Provenance Encoding

1. Introduction

Wireless Sensor Network (WSN)

Wireless Sensor Network (WSN) is deployed to monitor the physical environment, process sensing information, and report to the sink through wireless communications. Sensor nodes are typically resource constrained micro-electronic devices. This necessitates effective solutions in various aspects of WSNs, such as routing, medium access control, duty cycle scheduling, etc. Such types of sensor nodes could be deployed in home, military, science, and industry.

We propose a provenance encoding strategy whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter 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. As opposed to existing research that employs separate transmission channels for data and provenance [4], we only require a single channel for both. Furthermore, traditional provenance security solutions use intensively cryptography and digital signatures [5], and they employ append-based data structures to store provenance, leading to prohibitive costs. In contrast, we use only fast Message Authentication Code (MAC) schemes and Bloom filters (BF), 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.

Our specific contributions are:-

• 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.
2. Related Work

Network accountability and failure analysis is important for network management. It also described the need of network provenance. The paper [1] proposed ExSPAN provenance system in distributed environment. ExSPAN used data provenance to prove the state of the network. ExSPAN was developed using rapid net which is based on ns3 toolkit. Experimental results showed that the system is generic and extensible. Same as Pedigree this scheme also did not consider security of the provenance data.

[2] W. Zhou et.al proposes “Querying and Maintenance of Network Provenance at Internet- Scale” which describes the history and sub part of the network state. This result came from the execution of a distributed protocol. The disadvantage of this system is also does not address security concerns and is specific to some network use cases.

[3] Zhou, et.al, proposes a “Secure Network Provenance.”. This extends network provenance up to the adversarial environments. Even though all of these systems are general purpose network provenance systems but they are not optimized for the resource constrained sensor networks

[4] A. Syalim et al propose a “Preserving Integrity and Confidentiality of a Directed Acyclic Graph Model of Provenance.”. The chain model of provenance ensure integrity(no one can change the data other than the original user) and confidentiality(no one can see the data other than original user)through encryption, checksum and incremental chained signature mechanism. Syalim et al. extend this method by applying digital signatures. This signature applied to a DAG model of provenance.

The another paper focused on provenance management and proposed a novel secure provenance transmission scheme in which provenance is embedded into inter packet timing domain[5] and paper also considered limitations, requirements of WSN. Proposed scheme is different from traditional watermarking schemes. The scheme embeds provenance data into inter packet delays and not in actual sensor data. As provenance data is not directly embedded into actual data, data quality degradation issue is solved. Provenance information is recovered using optimal threshold bases mechanism to reduce the provenance recovery errors. Proposed scheme is based on the spread spectrum watermarking technique and it is efficient against various sensor network or flow watermarking attacks. This scheme assumes that provenance data remains same for flow of the packets.

3. System Architecture

The figure 1 shows the system architecture. 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.

3.1 Use Case Diagram

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.
4. Detecting Packet Drop Attacks

Mechanism

Data Packet Representation
To enable packet loss detection, a packet header must securely propagate the packet sequence number generated by the data source in the previous round. In addition, as in the basic scheme, the packet must be marked with a unique sequence number to facilitate per-packet provenance generation and verification. Thus, in the extended provenance scheme, any jth data packet contains (i) the unique packet sequence number (seq[j]), (ii) the previous packet sequence number (pSeq), (iii) a data value, and (iv) provenance.

Provenance Encoding
Figure 1 depicts the extended provenance encoding process. The provenance record of a node includes (i) the node ID, and (ii) an acknowledgement of the lastly observed packet in the flow. The acknowledgement can be generated in various ways to serve this purpose.

Provenance Decoding at the BS
Not only the intermediate nodes, but also the BS stores and updates the latest packet sequence number for each dataflow. Upon receiving a packet, the BS retrieves the preceding packet sequence (pSeq) transmitted by the source node from the packet header, fetches the last packet sequence for the flow from its local storage (pSeqb), and utilizes these two sequences in the process of provenance verification and collection.

5. Implementation

There are four modules in the implementation

A. Network Model
We consider a multi-hop wireless sensor network, consisting of a number of sensor nodes and a base station that collects data from the network. Sensor nodes are stationary after deployment, but routing paths may change over time, e.g., due to node failure. Each node reports its neighbouring (i.e., one hop) node information to the BS after deployment. The BS assigns each node a unique identifier node ID and a symmetric cryptographic key. In addition, a set of hash functions are broadcast to the nodes for use during provenance embedding.

We assume a multiple-round process of data collection. Each sensor generates data periodically, and individual values are aggregated towards the BS using any existing hierarchical (i.e., tree-based) dissemination scheme.

B. Provenance Encoding
We consider node-level provenance, which encodes the nodes at each step of data processing. We assume that the BS is trusted, but any other arbitrary node may be malicious. An adversary can eavesdrop and perform traffic analysis anywhere on the path. In addition, the adversary is able to deploy a few malicious nodes, as well as compromise a few legitimate nodes by capturing them and physically overwriting their memory.

C. Provenance Decoding
When the BS receives a data packet, it executes the provenance verification process, which assumes that the BS knows what the data path should be, and checks the iBF to see whether the correct path has been followed. However, right after network deployment, as well as when the topology changes (e.g., due to node failure), the path of a packet sent by a source may not be known to the BS.

In this case, a provenance collection process is necessary, which retrieves provenance from the received iBF and thus the BS learns the data path from a source node. Afterwards, upon receiving a packet, it is sufficient for the BS to verify its knowledge of provenance with that encoded in the packet.

D. Detecting Packet Drop Attacks
We extend the secure provenance encoding scheme to detect packet drop attacks and to identify malicious node. We assume the links on the path exhibit natural packet loss and several adversarial nodes may exist on the path. For simplicity, we
consider only linear data flow paths. Also, we do not address the issue of recovery once a malicious node is detected. Existing techniques that are orthogonal to our detection scheme can be used, which may initiate multipath routing or build a dissemination tree around the compromised nodes.

6. Performance Evaluation

Figure 3. Packet Drop
The above figure 3 shows the packets drop. Here the three cases are considered. The red line, blue line and the green line are the three considerations.

Figure 4. False Positive Rate
The figure 4 depicts the false positive rate when provenance verification fails.

Figure 5. Collection Error
The figure 5 shows the collection error which depends on BF packet size.

7. Conclusion and Future Work
The scheme ensures confidentiality, integrity and freshness of provenance. 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. 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


