Dictionary Based Secure Provenance Compression for Wireless Sensor Network

#1Mr. Ajit M. Karanjkar, #2Prof. D.H. Kulkarni

#1Department of Computer Engineer, SMT. Kashibai Navale College of Engineering, Pune, India
#2Professor, Department of Computer Engineer, SMT. Kashibai Navale College of Engineering, Pune, India

ABSTRACT

Due to energy and bandwidth limitations of wireless sensor networks (WSNs), it is crucial that data provenance for these networks be as compact as possible. Even if lossy compression techniques are used for encoding provenance information, the size of the provenance increases with the number of nodes traversed by the network packets. To address such issues, we propose a dictionary based provenance scheme. In our approach, each sensor node in the network stores a packet path dictionary. With the support of this dictionary, a path index instead of the path itself is enclosed with each packet. Since the packet path index is a code word of a dictionary, its size is independent of the number of nodes present in the packet’s path. Furthermore, as our scheme binds the packet and its provenance through an AM-FM sketch and uses a secure packet sequence number generation technique, it can defend against most of the known provenance attacks. Through simulation and experimental results, we show that our scheme outperforms other compact provenance schemes with respect to provenance size, robustness, and energy consumption.

Index Terms: Provenance, dictionary based compression, sensor network.

I. INTRODUCTION

Large scale Wireless sensor networks are deployed in numerous application domains, including medical monitoring, environmental monitoring, surveillance, home security, military operations, industrial machine monitoring, etc. In to this application domains, sensors vary from miniature, body-worn sensors to external sensors such as video cameras or positioning devices. Since provenance records the history of both data acquisition and transmission, it is considered as an effective mechanism to evaluate the trustworthiness of data. It provides the information about the operations performed on data. However, reducing the size of the provenance is crucial in large-scale sensor networks. Wireless Sensor nodes in these networks may not be able to record and manipulate very large provenance data due to storage and computational resource constraints. Beside, Transmission channels may not have sufficient capacity for transmitting large provenance data.

We have investigate the problem of efficient and secure compression of provenance information in wireless sensor networks (WSNs). The problem imposes a set of challenges:

- The compression of provenance should be as compacts possible so that for large-scale WSNs the provenance size does not increase with the number of nodes traversed by the network packets.
- The compression or encoding should ensure that the system does not lose any provenance information after decoding.
- The trustworthiness of the provenance must be assured.

To reduce the provenance size for large-scale Wireless Sensor Networks, earlier approaches use lossy compression techniques. For example, some provenance schemes only record the data processing or routing nodes, but discard the order in which they are traversed by the network packets. This approaches fail to provide accurate path provenance of data packets. On the other hand, if a model randomly generates a message, according to Shannon’s theory the message cannot be encoded into a smaller number of bits (on average) than the entropy of that model. The Entropy is a measure of the uncertainty in a random variable which quantifies the expected value of the information contained in a message so, the theorem sets a lower bound on the size of provenance for an entropy based model.
Hence, transmission channels do not experience difficulties with handling provenance data in large scale Wireless Sensor Network. Furthermore, our compression scheme is lossless in contrast to other lightweight mechanisms which are lossy in nature. The simulation and experimental results of our dictionary based lossless compression approach show that it generates provenance of much smaller size than that of existing lossy provenance schemes.

II. MOTIVATION

Secure Provenance Compression management for sensor networks introduce several challenges such as low energy and bandwidth consumption, efficient storage and secure transmission. There are numerous techniques and method proposed for confidentiality, integrity, and trustworthy of secure provenance transmission in WSN.

The feasibility of the asymmetric key management has been shown in Wireless Sensor Networks recently, which compensates the shortage from applying the symmetric key management for security.

Distributed system which evaluates the trust in the network that is more flexible and more responsive, which enhance the network trust in network.

III. LITERATURE SURVEY


In this paper data are produced at a large number of sensor node sources and processed in network.


In this paper develop a light weight scheme for securely transmitting provenance for sensor network.


In this article Lightweight provenance encoding and decoding scheme based on bloom filters.


In this paper is Evaluated a SNooPy prototype with three different example applications: the Quagga BGP daemon, a declarative implementation of Chord, and HadoopMapReduce.


In this paper we adapt the probabilities packet marketing (PPM) approach trace back. Further two encoding methods and combine to deal with topological changes in the network.

IV. EXISTING SYSTEM

A secure packet sequence number generation mechanism is introduced and use the AM-FM sketch technique to secure the provenance. Some provenance schemes only record the data processing or routing nodes, but discard the order in which they are traversed by the network packets.

V. OBJECTIVES

- Each sensor node in the network stores a packet path.
- The goal of the proposed dictionary based secure Provenance for WSNs is to guarantee a secure and efficient data transmission between two nodes.
- The trustworthiness of the provenance.
- Increase accuracy and reliability.
- Increase the lifetime of the sensor node and reduces the energy consumption.
- Data security.
- The major objective of data aggregation is to bring together and aggregate data in an energy efficient way so that network lifetime is enhanced.

Transmission of data in efficient and secure way. Proposed a dictionary based provenance scheme which is the most compact and lossless scheme up to date.

VI. PROPOSED SYSTEM

In order to address the drawbacks of lossy compression techniques and to address the limitation of entropy lower bound, a dictionary based approach is proposed to encode the sensor data provenance. Proposed technique compresses the packets’ paths and represents those using distinct indexes. This indexes are stored in a dictionary. With the
support of this dictionary, a fixed size path index can be used to represent a path of arbitrary length. This indexes are stored in a dictionary. The use of dictionary based method allows one to keep the size of a compressed path smaller than the path’s entropy at the cost of additional storage space for dictionaries. Efficient, and distributed data algorithm for encoding the provenance information as well as a centralized approach for its decoding. A secure packet sequence number generation mechanism is introduced and use the AM-FM sketch technique to secure the provenance.

VII. PROPOSED METHODOLOGY

4.1 System Model

We also present the provenance model along with some useful concepts that are used in our proposed scheme.

Due to energy and bandwidth limitations of WSNs(wireless sensor networks), it is crucial that data provenance for these networks be as compact as possible. The lossy compression techniques are used for encoding provenance information, the size of the provenance increases with the number of nodes traversed by the network packets. To address such issues in dictionary based, we propose a dictionary based provenance scheme. In our approach, each sensor node in the network stores a packet path dictionary, with the support of this dictionary, a path index instead of the path itself is enclosed with each packet. The packet path index is a code word of a dictionary, its size is independent of the number of nodes present in the packet’s path.

Moreover, as our scheme binds the packet uses a secure packet sequence number generation technique, it can defend against most of the known provenance attacks. Through simulation and experimental results, we show that our scheme outperforms other compact provenance schemes with respect to provenance size, robustness, and energy consumption.

4.1.1 Network Model

The BS assigns each node a unique identifier in a counter counti, and an encryption key ki that is shared between the BS and that particular node. Routing paths may change over time due to node failure, mobility, link quality degradation, etc. Hence, our model supports both stationary and dynamic natures of sensor networks.

4.1.2 Data Model

The sensor nodes in a network generate data periodically. We name these nodes as data source nodes. A node may also receive data from another node in order to forward such data towards the BS. We call this node a forwarder node. Each packet contains used in Dictionary Based secure provenance in WSNs: (i) packet’s sequence number, (ii) its source node’s ID i.e., the ID of the node that generates the packet, (iii) data value, (iv) provenance record, and (v) message authentication code (MAC).

Provenance Model: - Network data provenance. The provenance of a data packet p is represented as a graph T(Vp,Ep), referred to as provenance graph.

Dictionary index: - Dictionary index (dicIndex) is used to represent the compression of a linear path.

Packet path index: - Assume that a packet p traverses the path [nM ;n M-1, . . . , n1} to reach the BS.

4.2 Provenance Scheme

Develop a distributed mechanism to encode provenance at sensor nodes and a centralized approach to decode provenance at the Base Station (BS). The protection against any unauthorized modification, the packet and its
provenance are bound together by a secure message authentication code. The Base Station (BS) verifies the MAC and then extracts the provenance graph for the packet it receives.

4.2.1 Provenance Encoding
A data packet, provenance encoding refers to the creation of compressed provenance at each node on the packet’s path. During the process of provenance encoding, each node along a packet’s path is assumed to be one of these three: 1) data source node, 2) forwarder node, and 3) aggregator node.

Algorithm 1: Provenance Encoding:

Input: (ni, seqi)
Output: prIndex=(v, pathIndex)
if ni is a data source node then
prIndex:v = vi
pp = ni
agr = φ;
prIndex.pathIndex = <ni, φ>
end if
if ni is a forwarder node then
prIndex:v = vi
pp = pp (U) ni
agr = φ;
prIndex.pathIndex = <nk, ni>
end if
if ni is an aggregator node then
prIndex:v = vi
pp = ni
agr = [seq1, seq2, . . . ; seqM]
prIndex.pathIndex = <nb1, ni, . . . ; nbM, ni>
end if

4.2.2 Provenance Binding
In Provenance Binding we approach provide traditional MAC schemes, e.g., MD5 or SHA-1, are designed for centralized scenarios. The packet’s path generates an independent MD5 or SHA-1. Provenance binding technique which is a direct application of the AM-FM sketch mechanism.

4.2.3 Provenance Decoding
When the Base Station (BS) receives a packet, it verifies the integrity of the protected data through the AM-FM evaluation process. If the verification confirms that the protected data are trustworthy, the Base Station (BS) accepts the packet, otherwise, the packet is dropped. For an accepted packet p, the provenance graph represented as T(Vp, Ep) is retrieved by looking up its path-Index in the Packet Path Dictionary (PPD) of the BS.

Algorithm 2: Provenance Decoding:

Input: prIndex = (v, pathIndex)
Output: T(Vp, Ep)
if the AM-FM verification fails then drop the received packet
else
if v:agr = φ then
T(Vp, Ep) = QuerypathIndex to PPD.
else
Y = number of ‘;’ inpathIndex+1
for i = 1 to Y do
pathi = Query branch i of pathIndex to PPD.
end for
T(Vp, Ep) = (path1; . . . ; pathY)
end if
end if

VIII. CONCLUSION
In this paper, we propose a dictionary based secure provenance scheme for wireless sensor networks. Using packet path dictionaries, we enclose path indexes instead of the path itself in the provenance. Hence, the size of the compressed provenance in our lossless approach is smaller than that of the existing lossy provenance schemes. By using the AM-FM sketch scheme and a secure packet sequence number generation technique, we ensure the security objectives of our scheme. Simulation and experimental results show that our scheme can save more energy and bandwidth than other existing provenance schemes.

REFERENCES


