Secure Routing Protocol Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks

Abin Thankachan[1], Snehal Merukar[2],Aliasgar Nadir[3], Pratik Warulkar[4], Pritesh A.Patil[5]
[1, 2, 3, 4, 5]Department of Information Technology
[1, 2, 3, 4, 5]All India ShriShivaji Memorial Society's Institute of Information Technology, SavitribaiPhule Pune University, Pune, India-411001

Abstract-*Wireless sensor networks collect the data from all nodes and which is used for the decision making purpose. Sometimes advisory node may introduce or compromise with the existing node so that the data can be easily altered. Data provenance verifies the sensor data. But some challenges occur while using provenance like space complexity, bandwidth consumption. In this proposed system a secure scheme is used to securely transmit provenance for sensor data. Here the scheme uses only the bloom filter logic to encode and decode the data provenance and also energy efficient routing protocol for saving the energy of the network. This Scheme extends the technique to find the packet drop attacks in the networks. In this proposed system,we noted the problem of securely transmitting provenance for sensor networks, and used the provenance encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance. Here this scheme is extended to in-corporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. At the end, project will evaluate the proposed technique both analytically and empirically.*

Keywords-Provenance, Security, Sensor Networks.

I. INTRODUCTION

Wireless sensors used to aggregate the data from the environment like temperature, humidity, etc. Which are required for the decision making by base station. Only trustworthy information is considered in the decision making process. In a multi-hop sensor network, data provenance allows the BS to trace the source and forwarding path of an individual data packet. Provenance must be recorded for each packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of sensor nodes.It is necessary to address security requirements such as confidentiality, integrity and freshness of provenance. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data. Data encoding technique is used to encode the data provenance at sender node.Data decoding algorithm which is used at the base station for verifying the data provenance i.e. the data is followed the same path or not, which is pre-decided by the sender node. Packet loss minimizes the Packet Delivery Ratio. Packet loss can because by a number of factors including signal degradation over the network medium due to multi-path fading. Packet loss is possible in wireless sensor network. So that the intruders can be easily capture the data. Identifying the dropping packet and misbehaving activities are the most necessary measures for secure transmission in it. Without a certificate a node cannot participate in the transmission. The technique also extended to find the data packet loss attack in the network.In provenance encoding each node on the path of a data packet securely attach 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.

The popularity of sensor networks and their many uses in critical domains such as military and healthcare make them more vulnerable to malicious attacks. In such contexts, trustworthiness of sensor data and their provenance is critical for decision-making. We present an efficient and secure approach for transmitting provenance information about sensor data. Our provenance approach uses light-weight in-packet Bloom filters that are encoded as sensor data travels through intermediate sensor nodes, and are decoded and verified at the base station.

II. LITERATURE SURVEY

Architecture

The following Fig a.will explain the provenance encoding at sensor node and provenance decoding process at base station.

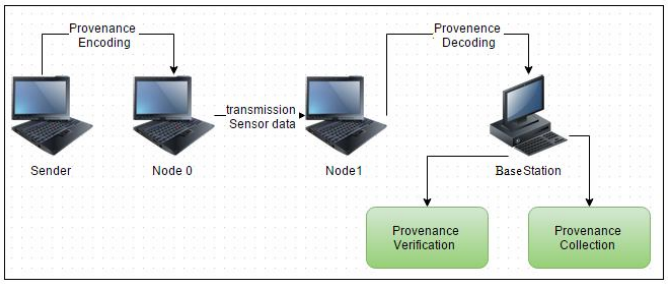

Fig a. System Architecture

In this fig a. the Sender sends data to intended receiver. As soon as data is send Provenance Encoding is done at Node 0 and transmission of this sensor data is done at Node 1 and Provenance Decoding process is performed at Base Station and Provenance collection and Provenance Verification is done at Base Station.

Project Life Cycle

The following Fig b. will explain Project Life Cycle.

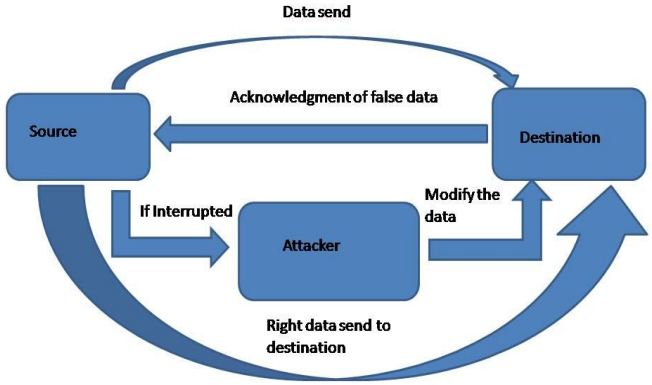

Fig b. Project Life Cycle

Project will be implemented in the following phases: -

1. Requirement analysis and planning

In this phase the requirement document was finalized along with the planning to implement feasible requirements and deadlines were decided accordingly.

2. Design

The purpose of this phase is to design encoding provenance and decoding mechanism that ensures security and performance guarantee.

3. Implementation

Implementation explains the methodology identified for development of the project.

4. Testing

Testing is carried by implementing the techniques such as unit bloom filter, AES, DES Algorithm.

5. Deployment

The project will be finalized as per the requirements and the end results with future work related to project.

III. CONCLUSION

This paper presented the provenance encoding and decoding scheme based on Bloom filters and addressed the problem of securely transmitting provenance for sensor networks. 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.

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] 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.

[4] M. Mitzenmacher, “Compressed bloom filters,” in Proc. of ACMSymp. on Principlesof Distributed Computing, 2001, pp. 144–150.