VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM
INDIA

"Jnanna Sagama", Belgaum-560014, Karnataka

A Project Synopsis
On

A Lightweight Secure Scheme for Detecting Provenance Forgery in Wireless Sensor Networks

Submitted by

SHIVARAJ BILGUNDI	[1DS12IS099]
SUDHANVA M U	[1DS12IS107]
SAGAR S	[1DS12IS086]
V VISHWAS AGARWAL	[1DS12IS115]

Research Guide

Ms. SHARON CHRISTA
Asst. Professor
B.E, M.Tech (Ph.D)

Affiliation

Department of Information Science and Engineering
Dayananda Sagar College of Engineering
Bangalore – 560078

A Lightweight Secure Scheme for Detecting Provenance Forgery in Wireless Sensor Networks

PROBLEM STATEMENT:

In a multi hop sensor networks, data provenance allows the base statement to trace the source and forwarding path of a data packet provenance must be recorded for all data packets but important challenge arise due to the tight storage, Energy and band with constrains. Therefore, it is necessary to devise a light weight Provence solution with low overhead.

Furthermore in an untrusted environment where there may be attacks. It is necessary to address security requirements such as confidentiality, integrity & freshness of Provenances.

The aim of the system is to design a provenance encoding mechanism that satisfies such security & performances needs.

MOTIVATION:

In the existing there are two separate transmission channels for data and provenance. We only want single channel for both. Furthermore, traditional provenance security solutions use intensively cryptography and digital signatures, and they employ append-based data structures to store provenance, leading to prohibitive costs.

OBJECTIVE AND SCOPE:

In our project, 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.

PROCESS AND DESCRIPTION:

Sensor networks are used 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 (BS) 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). Although provenance modeling, collection, and querying have been studied extensively for workflows and curated databases, provenance in sensor networks has not been properly addressed. We investigate the problem of secure and efficient provenance transmission and processing for sensor networks, and we use provenance to detect packet loss attacks staged by malicious sensor nodes.

The proposed technique relies on inpacket 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

COMPONENTS LIST:

➢ **Processor**	:	Itanium 7
➢ **Hard Disk**	:	1 TB
➢ **Monitor**	:	HDMI
➢ **RAM**	:	8 GB
➢ **Mouse**	:	Optical
➢ **Keyboard**	:	Multimedia

SOFTWARE’S USED:

➢ **Operating system**	:	Windows XP Professional / Windows7
➢ **Coding Language**	:	Java (Jdk 1.7),
➢ **Database**	:	My-SQL 5.0
➢ **Database GUI**	:	SQLYog
➢ **Eclipse tool**	:	Eclipse Indigo

CONTRIBUTION:

In proposed system using key exchanging, cryptography, and signature technique are used. So easily detect the suspicious data. In addition, we extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes.

CONCLUSION:

We addressed the problem of securely transmitting prove-nance 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 in-corporate 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.