MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

A SECURE MODEL FOR DETECTING ORIGIN FORGERY AND PACKET DROP ATTACKS IN WSN

Meghraj Kadam, Sagar Dakhore, Keshav Chavan, Amol Bandgar
Prof.Mandar Mokashi

Computer Engineering, Dr.D.Y.Patil School of Engineering,
Pune, India

Abstract-*The basic operation in such a network is the efficient gathering and transmission of sensed data to a base station for advance processing. The life of such a sensor system is the time during which we can gather information from all the sensors to the base station. A fundamental challenge in data gathering is to maximize the system lifetime, given the energy constraints. As sensor networks are being all the time more deployed in decision-making.*

The process that on in packet Bloom filters to encode provenance of the information. We introduce efficient tools for provenance verification method and reconstruction method at the base station with the functionality to detection packet drop attacks or by malicious data forwarding nodes. In our paper, we propose a novel lightweight scheme to securely transmit provenance for sensor data. We introduce efficient tools for provenance verification and reconstruction at the base station. In addition the secure provenance scheme with the functionality to detection packet drop attacks by malicious data from the source to destination node.

Keywords*: Provenance Mechanism, Security Mechanism, Wireless Sensor Networks. Bloom Filter mechanism, Distributed systems, Packet forwarding, inter-networking Sensor networks, Security.*

1. INTRODUCTION

Sensor networks are used in application domains, examples are cyber physical infrastructure, environmental monitoring, whether monitoring power grids, etc. The data that should be large sensor node sources and processed in-network with their way to a Base Station (BS) that performs which decision should be taking. Information is considered in the decision process or making. Data provenance is an effective method to assess data trustworthiness, and the actions performed on the data. Provenance in sensor networks has not been present properly addressed. We investigate the problem of secure and efficient

provenance transmission and handling for sensor networks, and we use provenance to detect packet loss attacks staged by malicious sensor nodes.

In a multi-hop sensor network the *data provenance is to* allow the Base Station to trace the source and forwarding path of a specific data packet the provenance must be record for each an every packet, but important challenges arise due to some reason the first is tight storage, energy and bandwidth constraints of sensor nodes. Therefore it is necessary devise a light-weight provenance solution with low overhead. Sensors should operate in untrusted environment, where they may be happens subject to attacks. That's why it is necessary to address security requirements such as *privacy*, *reliability* and *cleanness* of provenance. Our project goal is to design a *provenance encoding and decoding tool* that would be satisfies such safety and presentation needs. We Design propose a provenance encoding strategy where each node on the track of a data packet securely embeds provenance information within a *Bloom filter* that is conveyed along with the data. Receiving the packet the Base Station should be extracts and verifies the provenance information. The provenance encoding system that allows the Base Station to detect if a *packet drop attack* was staged by a malicious node.

We use fast Message Authentication Code and *Bloom filters (BF)*, which are stable size data structures that efficiently represent provenance. The modern developments in micro sensor technology and low power analog and digital electronics, have led to the development of distributed, wireless networks of sensor devices Sensor networks of the future are intended to consist of hundreds of cheap nodes, that can be readily deployed in physical situations to collect useful information.

Our motivation on the subsection of distributed networking applications created on packet-header-size Bloom filters to share some state between network nodes. The specific state carried in the Bloom filter differs from application to application, ranging from secure credentials to IP prefixes and link identifiers with the shared requirement of a fixed-size packet header data structure to well verify set memberships. Bloom filters make effective 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. LITERATURE SURVEY

An Efficient Clustering based Heuristic for Data Gathering and Aggregation in Sensor Networks-The base station and the available energy at each sensor, we are interested in finding an efficient manner in which the data should be collected from all the sensors and transmitted to the base station, such that the system lifetime is maximized. An Efficient

Clustering based Heuristic for Data Gathering and Aggregation in Sensor Networks-This is the maximum lifetime data gathering problem. An efficient clustering based heuristic to solve the data gathering problem. In-packet Bloom filters: Design and networking applications- We consider the design of such in packet Bloom filters (iBF).Compressed Bloom Filters-Introduce compressed Bloom filters, which improve performance when the Bloom filter is passed as a message and its transmission size is a limiting factor. Provenance based Trustworthiness Assessment in Sensor Networks-Our approach uses the SYNOPSIS data provenance as well as their values in com- putting trust scores, that is, quantitative measures of trustworthiness. Secure in-packet Bloom Filter forwarding- In-packet Bloom filters allow one to forward source-routed packets with minimal forwarding tables, the Bloom filter encoding the identities of the links the packet needs to be forwarded over. A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks-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.

3. NETWORK MODEL

We study a multi-hop wireless sensor network, containing of a number of sensor nodes and a base station that gathers data as of the network. The network is modeled as a graph G(N,L), where N = {ni|, 1 ≤ i ≤ |N|} is the set of nodes, and L is the fixed of links, containing an element li,j for each pair of nodes ni and nj that are communicating directly with each other. Each node reports its neighboring node information to the BS after deployment. The BS assigns each node a single identifier nodeID and a symmetric cryptographic key Ki. In addition, a set of hash functions H = {h1, h2, ...,hk} are broadcast to the nodes aimed at use during provenance embedding.

3.1 DATA MODEL

We adopt a multiple-round process of data collection. Each sensor makes data periodically, and individual values are combined near the BS using any existing hierarchical like tree-based dissemination scheme. A data path of D hops is represented as < nl, n1, n2, ..., nD >, where nlis a leaf node representing the data source, and node ni is i hops away from nl. Each non-leaf node in the

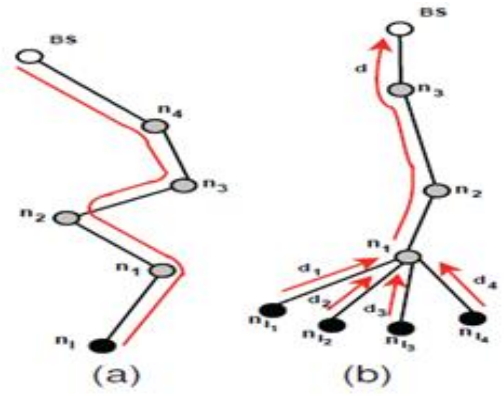

Fig.1: Provenace Graph

path collections the received data and provenance with its own locally-generated data and provenance. The data packet contains (i) a exclusive packet sequence number, (ii) a data charge, and (iii) provenance. The sequence number is involved to the packet by the facts source, and all nodes use the same sequence number for a given round.

3.2 PROVENANCE MODEL

Definition for Provenance: Given a data packet d, the provenance pd is a directed acyclic graph G(V,E) satisfying the following properties: pd is a sub graph of the sensor network G(N,L); for vi, vj ∈V , vi is a child of vj if and only if HOST (vi) = ni participated in the distributed calculation of d and/or forwarded the data to HOST (vj) =nj ;for a set U = {vi} ⊂V and vj ∈V ,U is a set of children of vj if and only if HOST (vj) collects processed/forwarded data from each HOST(vi ∈U) to generate the aggregated result.

4. SECURITY OBJECTIVES

1) Query-based systems: - In query-based systems, the base station the facts sink broadcasts a query to the network and the nodes respond with the important information. Messages from separate nodes are potentially aggregated enrooted to the base station. Lastly, the base station computes one or more collective values based on the messages it has received.

2) Event-based systems: - Nodes send a message to the base station only when the target event occurs in the area of interest. If different reports being spread correspond to the same event, they can be combined by an intermediate node on the route to the base station.

The Objectives Are:-

- Confidentiality: An adversary cannot gain any knowledge about data provenance by examining the contents of a packet. Only legal parties (e.g., the BS) can process and check the truth of provenance.
- Integrity: An adversary, stand-in alone or colluding with others, cannot add or remove non-colluding nodes from the provenance of benign data generated by benign nodes minus being detected.
- Freshness: An adversary cannot replay captured data and provenance without presence detected by the BS.

5. SYSTEM ARCHITECTURE:

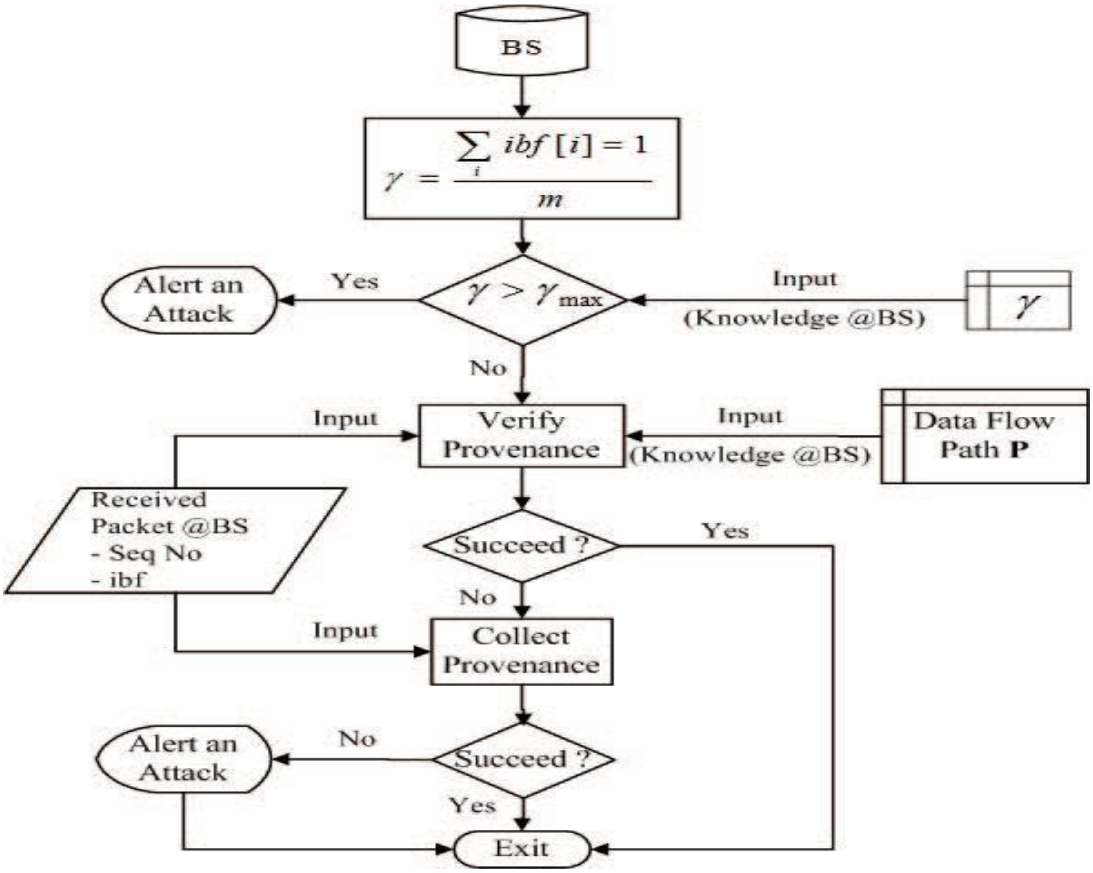

Fig.2: System Architecture

6. CONCLUSION

In this paper data should be of securely transmitting form the source node to destination in a sensor networks, and execution a light weight packet forwarding provenance encoding as well as decoding scheme by using the Bloom filters process. Our Objectives confidentiality, integrity and freshness of the provenance. The schema contains packet sequence information that supports detection of packet damage attacks. Experimental and evaluation results parameter showing that the future scheme is effective, light-weight and mountable. In Technique secure provenance scheme with the functionality to detection packet drop attacks by malicious data from the source to destination node.

ACKNOWLEGEMENT

Authors are cordially giving thanks to Prof. Mandar Mokashi for his valuable and constructive suggestions. We sincerely thank Head of Department (Computer Engineering) Prof. Soumitra S. Das for his reassuring encouragement throughout the preparation of our paper. Also thanking to all others who have tried hard to make their work easy to accomplish.

REFERENCES

[1]. *[1] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof sketches:Verifiable in-netwok aggregation," in ICDE, 2007, pp. 84–89.*

[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]. *A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in Proc. of IPSN, 2008, pp. 245–256.*

[4]. *S. Madden, J. Franklin, J. Hellerstein, and W. Hong, "TAG: a tiny aggregation service for ad-hoc sensor networks," SIGOPS Operating Systems Review, no. SI, Dec. 2002.*

[5]. *K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-aware storage systems," in Proc. of the USENIX Annual Technical Conf., 2006, pp. 4–4.*

[6]. *P. Jokela, A. Zahemszky, C. Esteve, S. Arianfar, and P. Nikander, "Lipsin: line speed publish/subscribe inter-networking," in Proc. Of ACM SIGCOMM, 2009, pp. 195–206.*