International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

A Secure Scheme for Sensing Background Forgery and Packet Dropattacks in WSN

[1]Mr P. SURESH, [2] Mrs. N.SUJATHA

[1] Pursuing M.Tech(CSE)from Jagruti Institute of Engineering and Technology
[2] Associate Professor, Department of Computer Science and Engineering,
Jagruti Institute of Engineering and Technology, Telangana State, 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. 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*

Keywords: *Provenance Mechanism, Security Mechanism, Wireless Sensor Networks. Bloom Filter mechanism, Distributed systems, Packet forwarding, Wireless Sensor Network, Encryption, Decryption.*

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 secure and efficient provenance transmission and processing for sensor networks. In a multi-hop sensor network, data provenance allows the base station to trace the source and forwarding path of an individual data packet since its generation. Provenance must be recorded for each data packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of the sensor nodes. Therefore, it is necessary to devise a light-weight provenance solution which does not introduce significant overhead. Furthermore, sensors often operate in an untrusted environment, where they may be subject to attacks. Hence, it is necessary to address security requirements such as confidentiality, integrity and freshness of provenance. Our goal is to design a provenance encoding and decoding mechanism that satisfies such

security and performance needs. We propose a provenance encoding strategy whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter, which is transmitted along with the data. Upon receiving the data, the base station extracts and verifies the provenance. 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 [1] 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 [2], [3], 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. 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. Therefore, it is necessary to devise a light-weight provenance solution with low overhead. Furthermore, sensors often operate in an untrusted environment, where they may be subject to attacks. Hence, it is necessary to address security requirements such as confidentiality, integrity and freshness of provenance. Our goal is to design a provenance encoding and decoding mechanism that satisfies such security and performance needs. 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

2. BACKGROUND

A. Network Model We have create a multihop wireless sensor network, consisting of a number of sensor node and a base station that collects data from the network. The networks is modeled as a graph G(N, L), where N = {n i |, 1 ≤ i ≤ |N |} is the set of nodes, and L is the set of link, containing an element l i,j for each pair ofnodes n i and n j that are communicating directly with each other. The Base station assigns each node a unique identifier nodeID and a symmetric cryptographic key K i .

B. Data Model We consider a multiple-round process of collecting data. Each sensor generates data periodically, and individual values areaggregated towards the Base station using any existing hierarchical dissemination scheme . Each data packet contains of (i) a unique packet sequence number, (ii) a data value, and (iii) provenance.

C. Threat Model It is also important to provide Data-Provenance Binding i.e., a coupling between data and provenance so that an attacker cannot successfully drop or alter the legitimate data while retaining the provenance, or swap the provenance of two packets.

D. the Bloom Filter (BF) Several BF variations that provide additional functionality exist. A Counting

Bloom Filter (CBF) associates a small counter with every bit, which is incremented/decremented upon item insertion/deletion. To answer approximate set membership queries, the distance sensitive Bloom filter has been proposed. However, aggregation is the only operation needed in our problem setting. The cumulative nature of the basic BF construction inherently supports the aggregation of BFs of a same kind, so we do not require CBFs or other BF variants.

We use only fast message authentication code (MAC) method and Bloom filter, which are fixed-size data structures that represent provenance. Bloom filters make best usage of bandwidth, and they yield low error rates in practice.We formulate the problem of secure provenance transmission in wireless sensor networks, and identify the challenges specific to this context. We propose an iBF (inpacket Bloom filter) provenance encoding mechanism also design efficient techniques for provenance decoding and verification at the base station. We extend the secure provenance encoding mechanism and devise a mechanism that detects data packet drop attacks step by malicious forwarding sensor nodes. We perform a detailed security analysis and performance evaluation of the proposed provenance encoding scheme and data packet loss detection mechanism.

3. DETECTING PACKET DROP ATTACKS MECHANISM

We extend the secure provenance encoding scheme to detect packet drop attacks and to identify malicious node(s). 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 (i.e., as illustrated in Fig. 1(a)). 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 [6] or build a dissemination tree around the compromised nodes [17]. We augment provenance encoding to use a packet acknowledgementthat requires the sensors to transmit more meta-data. For a data packet, the provenance record generated by a node will now consist of the node ID and an acknowledgement in the form of a sequence number of the lastly seen (processed/forwarded) packet belongingto that data flow. If there is an intermediate packet drop, Some nodes on the path do not receive the packet. Hence,during the next round of packet transmission, there will bea mismatch between the acknowledgements generated fromdifferent nodes on the path. We utilize this fact to detectthe packet drop attack and to localize the malicious node.We consider a data flow path P where nlis the only datasource. We denote the link between nodes niand n(i+1)as li. We describe next packet representation, provenanceencoding and decoding for detecting packet loss.

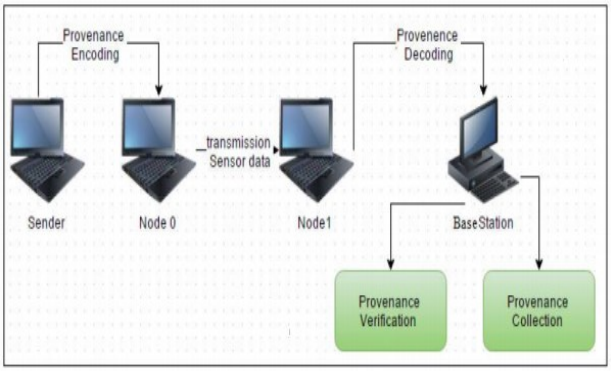
1. Data Packet Representation:

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 jthdata packet contains (i) the unique packet sequence number (seq[j]), (ii) the previous packet sequence number (pSeq), (iii) a data value, and (iv) provenance.

2. Provenance Encoding Fig. 4 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.

3. 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.

4. SYSTEM ARCHITECTURE



ExplanationSensor 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.

5. 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.

REFERENCES

[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.

[7] B. Carbunar, I. Ioannidis and C. Nita-Rotaru. JANUS: Towards Robust and Malicious Resilient Routing in Hybrid Wireless Networks. WiSe 2004, pp. 11-20.

[8] S. Sultana, M. Shehab, E. Bertino. Secure Provenance Transmission for Streaming Data. SUBMITTED in IEEE Transaction on Knowledge and Data Engineering (TKDE), 2011.

[9] Groth, P., Jiang, S., Miles, S., Munroe, S., Tsasakou, S., Moreau, L.: An architecture for provenance systems.(Nov. 2006)

[10] Buneman, P., Khanna, S., Tan, : Why and where: A characterization of data provenance. In: ICDT. (2001) 316–330

[11] Hasan, R., R., Winslett, M.: Preventing history forgery with secure provenance. ACM Transactions on Storage 5(4) (December 2009) 12:1–12:43

[12] Hasan, R., Sion, M .: The case of the fake picasso: Prevent against history forgery with secure provenance. In: FAST. (2009) 1–14

ABOUT THE AUTHORS

Mr P. SURESH is pursuing M.Tech degree in, Computer Science and Engineering from Jagruti Institute of Engineering and Technology, Telangana State, India.

Mrs.N.SUJATHA is presently working as Associate Professor in, Department of computer science and engineering, Telangana State,India.She has published several research papers in both International and National conferences and Journals.