Innovative Science and Technology Publications

International Journal of Future Innovative Science and Technology
ISSN: 2454- 194X Volume - 2, Issue - 2

Manuscript Title

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

Dr. P.Sumitra[1], P.Ponkavitha [2]

[1]Assistant Professor, Department of Computer Science

[2]Research Scholar, Department of Computer Science,

Vivekanandha College of Arts and Sciences for Women (Autonomous)

Elayampalayam, Tiruchengode India

E-Mail: prrkavi.91@gmail.com

May – 2016

www.istpublications.com

International Journal of Future Innovative Science and Technology, ISSN: 2454- 194X
Volume-2, Issue-2, May - 2016 editor@istpublications.com

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

Dr. P.Sumitra[1], P.Ponkavitha [2]

[1]Assistant Professor, Department of Computer Science
[2]Research Scholar, Department of Computer Science,
Vivekanandha College of Arts and Sciences for Women (Autonomous)
Elayampalayam, Tiruchengode India
E-Mail: prrkavi.91@gmail.com

ABSTRACT

Large-scale sensor networks are deployed in numerous application domains, and the data they collect are used in decision-making for critical infrastructures. Data are streamed from multiple sources through intermediate processing nodes that aggregate information. A malicious adversary may introduce additional nodes in the network or compromise existing ones. Therefore, assuring high data trustworthiness is crucial for correct decision-making. Data provenance represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. In this paper, we propose a novel lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on in-packet 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.

Index Terms—Provenance, security, sensor networks, Bloom Filters, Lightweight Secure Provenance Scheme.

I. INTRODUCTION

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 modelling, collection, and querying have been studied extensively for workflows and curate 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 entrusted 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 (BF) 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, 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. Our specific contributions are:

- We formulate the problem of secure provenance transmission in sensor networks, and identify the challenges specific to this context.
- We propose an in-packet Bloom filter (iBF) provenance encoding scheme.
- We design efficient techniques for provenance decoding and verification at the base station.
- We extend the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.
- We perform a detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism.

The rest of the paper is organized as follows: Section 2 setsthe problem background and describes the system threatand security models. Section 3 introduces the provenance encoding scheme, whereas Section 4 outlines the scheme extension and the mechanism for identification of malicious nodes that stage packet drop attacks. Section 5 presents the security analysis of our methods. Section 6 provides an analytical performance evaluation, whereas Section 7 presents the experimental evaluation results for the proposed scheme. We survey related work in Section 8 and conclude with directions for future research in it.

II BACKGROUND AND SYSTEM MODEL

In this section, we introduce the network, data and provenance models used. We also present the threat model and security requirements. Finally, we provide a brief primer on Bloom filters, their fundamental properties and operations.

A. Network Model

We consider a multichip wireless sensor network, consisting of a number of sensor nodes and a base station that collects data from the network.

The network is modelled as a graph GðN; LÞ, where N ¼ fn i j; 1 _ i _ jNjg is the set of nodes, and L is the set of links, containing an element li;j for each pair of nodes ni and nj that are communicating directly with each other. Sensor nodes are stationary after deployment, but routing paths may change over time, e.g., due to node failure.

Each node reports its neigh boring (i.e., one hop) node information to the BS after deployment. The BS assigns each node a unique identifier node ID and a symmetric cryptographic key Ki. In addition, a set of hash functions H ¼ fh1; h2; . . . ; hkg are broadcast to the nodes for use during provenance embedding.

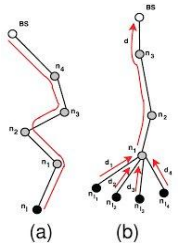

Fig :1 Provenance graph for a sensor network.

B. Data Model

We assume a multiple-round process of data collection. Each sensor generates data periodically, and individual values are aggregated towards the BS using any existing hierarchical (i.e., tree-based) dissemination scheme [6]. A data path of D hops is represented as <nl; n1; n2; . . . ; nD >, where nl is a leaf node representing the data source, and node ni is i hops away from nl. Each non-leaf node in the path aggregates the received data and provenance with its own locally-generated data and provenance.

C. Provenance Model

We consider node-level provenance, which encodes the nodes at each step of data processing. This representation has been used in previous research for trust management [1] and for detecting selective forwarding attacks [8]. Given packet d, its provenance is modelled as a directed acyclic graph GðN;LÞ where each vertex v 2 V is attributed to a specific node HOSTðvÞ ¼ n and represents the provenance record (i.e., nodeID) for that node. Each vertex in the provenance graph is uniquely identified by a vertex ID (VID) which is generated by the host node using cryptographic hash functions. The edge set E consists of directed edges that connect sensor nodes.

D. Threat Model and Security Objectives

We assume that the BS is trusted, but any other arbitrary Node may be malicious. An adversary can eavesdrop and perform traffic analysis anywhere on the path. In addition, the adversary is able to deploy a few malicious nodes, as well as compromise a few legitimate nodes by capturing them and physically overwriting their memory. If an adversary compromises a node, it can extract all key materials, data, and codes stored on that node. The adversary may drop, inject or alter packets on the links that are under its control. We do not consider denial of service attacks such as the complete removal of provenance, since a data packet with no provenance records will make the data highly suspicious [5] and hence generate an alarm at the BS. Instead the primary concern is that an attacker attempts to misrepresent the data provenance. Our objective is to achieve the following security properties: Confidentiality. An adversary cannot gain any knowledge about data provenance by analyzing the contents

of a packet. Only authorized parties(e.g., the BS) can process and check the integrity of provenance.

Integrity. An adversary, acting alone or colluding with others, cannot add or remove non-colluding nodes from the provenance of benign data (i.e., data generated by benign nodes) without being detected Freshness. An adversary cannot replay captured data and provenance without being detected by the BS. 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. Although this problem is orthogonal to the method we propose, we address it in Section 3.3.

E. The Bloom Filter

The BF is a space-efficient data structure for probabilistic representation of a set of items S = fs1; s2; . . . ; sng using an array of m bits with k independent hash functions h1; h2; . ; hk. The output of each hash function hi maps an item uniformly to the range [0, m _ 1], i.e., an index in a m-bit array. The BF can be represented as fb0; . . . ; bm_1g. Initially all m bits are set to 0. To insert an element s 2 S into a BF, s is hashed with all the k hash functions producing the values hiðsÞð1 _ i _ kÞ. The bits corresponding to these values are then set to 1 in the bit array.

To query the membership of an item s0 within S, the bits at indices hiðs0Þð1 _ i _ kÞ are checked. If any of them is 0, then certainly s0 62 S. Otherwise, if all of the bits are set to 1, s0 2 S with high probability. There exists a possibility of error which arises due to hashing collision that makes the elements in S collectively causing indices hiðs0Þ being set to 1 even if s0 62 S. This is called a false positive. Note that, thereis no false negative in the BF membership verification. Several BF variations that provide additional functionality exist. A counting bloom filter (CBF) [9] 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 [10] 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 aggregationof BFs of a same kind, so we do not require CBFs orother BF variants.

III SECURE PROVENANCE ENCODING

We propose a distributed mechanism to encode provenance at the nodes and a centralized algorithm to decode it at the BS. The technical core of our proposal is the notion of inpacket Bloom filter [11].

Each packet consists of a unique sequence number, data value, and an iBF which holds the provenance. We emphasize that our focus is on securely transmitting provenance to the BS.

In an aggregation infrastructure, securing the data values is also an important aspect, but that has been already addressed in previous work (e.g., [12]). Our secure provenance technique can be used in conjunction with such work to obtain a complete solution that provides security for data, provenance and data-provenance binding.

A . Provenance Encoding

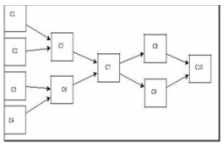

Fig 2 : Provenance graph

The Figure shows that to produce the final result, the contributor C5 uses the outputs of contributors C1 and C2while contributor of C6 uses the output of contributors C3 and C4. Contributor C7 uses the output of C5 and C6 which later used by C8 and C9. C10 is the final process is executed by that processes the outputs of C8 and C9. After each process is executed and the provenance of the process we had created/generated, the provenance is stored in the provenance database. All paragraphs must be indented. All Paragraphs must be justified, i.e. both left-justified and right -justifies.

B. Provenance Decoding

When a Base station receives a data packet .Base station know what the data packet should be checks. Afterwards, upon receiving a packet, it is sufficient for the BS to verify its knowledge of provenance with that encoded in the packet.

C. Provenance Verification

In verify modules following process are preformed.

1. Key generation
2. decryption
3. key exchanging
4. send to receiver module

Setup: The data producer sets up its signing key k and data consumer sets up its verification key k0 in a secure fashion that prevents malware from accessing the secret keys.

Sign(D, k): The data producer signs its data D with a secret key k, and outputs D along with its proof sign.

Verify(sig, D, k0): The data consumer uses key k0 to verify the signature sig of received data D to ensure its origin, and rejects the data if the verification fails.

IV IMPLEMENTATION

A. Secure Provenance Encoding

We secure provenance technique can be used in conjunction with such work to obtain a complete solution that provides.

The data is encoded and divided into multiple shares and then sent to the BS via different routes. However, these methods cannot identify the malicious node. They increase the network flow significantly, hence are not suitable for the resource constrained sensor networks. Additionally, these mechanisms could be vulnerable to route discovery attacks that prevent the discovery of non-adversarial paths.

V .DETECTING PACKET DROP ATTACKS

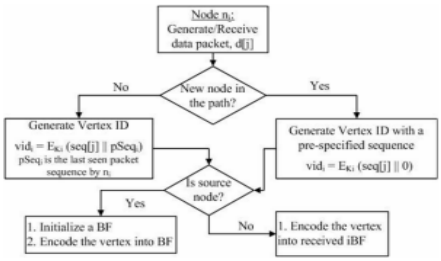

Fig : Extended provenance framework to detect packet drop attacks and identify malicious nodes.

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. 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 or build a dissemination tree around the compromised nodes.

VI. RELATED WORK

There has been a lot of research efforts to explore various mechanisms for handling the malicious data drop attack.These mechanisms can be classified into the following categories multipath routing protocols, acknowledgement based mechanisms, protocols using specialized hardware.The multipath routing protocols first discover multiple Paths for data forwarding and then uses these paths to Provide redundancy in the data transmission from a source. The data is encoded and divided into multiple shares and then sent to the BS via different routes. However, these methods cannot identify the malicious node. They increase the network flow significantly, hence are not suitable for the resource constrained sensor networks. Additionally, these mechanisms could be vulnerable to route discovery attacks that prevent the discovery of non-adversarial paths.

VII. CONCLUSIONS

In this paper, we have described our early implementation for a source-routing-based forwarding mechanism that is resistant to forwarding-identifier-guessing attacks.In this paper we addressed the problem of securely transmitting provenance for sensor networks, and proposed a lightweigh tprovenance encoding and decoding schemebased 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 prove that the proposed scheme is effective and scalable. In future work, we plan to implement a real system prototype of our.

REFERENCES

[1] H. Lim, Y. Moon, and E. Bertino, “Provenance-Based TrustworthinessAssessment in Sensor Networks,” Proc. Seventh Int’l WorkshopData Management for Sensor Networks, pp. 2-7, 2010.

[2] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, “Chimera: A VirtualData System for Representing, Querying, and Automating DataDerivation,” Proc. Conf. Scientific and Statistical Database Management,pp. 37-46, 2002.

[3] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer,“Provenance-Aware Storage systems,” Proc. USENIX Ann. TechnicalConf., pp. 4-4, 2006.

[4] Y. Simmhan, B. Plale, and D. Gannon, “A Survey of Data Provenancein E-Science,” ACMSIGMODRecord, vol. 34, pp. 31-36, 2005.

[5] R. Hasan, R. Sion, and M. Winslett, “The Case of the FakePicasso: Preventing History Forgery with Secure Provenance,”Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14,2009.

[6] S. Madden, J. Franklin, J. Hellerstein, and W. Hong, “TAG: A TinyAggregation Service for Ad-Hoc Sensor Networks,” ACM SIGOPSOperating Systems Rev., vol. 36, no. SI, pp. 131-146, Dec. 2002.

[7] K. Dasgupta, K. Kalpakis, and P. Namjoshi, “An Efficient ClusteringBased Heuristic for Data Gathering and Aggregation in Sensor Networks,” Proc. Wireless Comm. and Networking Conf., pp. 1948- 1953, 2003.

[8] S. Sultana, E. Bertino, and M. Shehab, “A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks,” Proc. Int’l Conf. Distributed Computing Systems (ICDCS) Workshops, pp. 332-338, 2011. [9] L. Fan, P. Cao, J. Almeida, and A.Z. Broder, “Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol,” IEEE/ACM Trans. Networking, vol. 8, no. 3, pp. 281-293, June 2000.

[10] A. Kirsch andM. Mitzenmacher, “Distance-Sensitive BloomFilters,”Proc.Workshop Algorithm Eng. And Experiments, pp. 41-50, 2006.