ISSN:0975-9646
Rupali Adhau et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4397-4399

Detecting Attacks in Wireless Sensor Network through Bloom Filtering

Rupali Adhau[#1], Ashwini Ambekar[*2], Abhishek Drakshe[*3], Rajat Thorave[#4]

[#]*Asst.Professor,Department of CE,Pune University,India*

[*]*BE.Student,Department of CE,Pune University,India*

Dr.D.Y.Patil Institute of Engineering and Technology Ambi,Pune,India

***Abstract*— In this paper, we describe our early implementation and testing of an in-packet Bloom filters forwarding node that implements cryptographically computed link identifiers. We have tested two different cryptographic techniques for the link-identity computation and thereby for making the forwarding decision. In-packet Bloom filters allow only one to forward source-routed packets with minimal forwarding tables. The Bloom filter encoding the identities of the links the packet need to be forwarded over. As sensor networks are being increasingly deployed in the decision-making infrastructures such as battlefield monitoring systems, SCADA making decision makers aware of the trustworthiness of the collected data is a crucial.**

In short paper describes how to preserve integrity and confidentiality of a directed acyclic graph model of provenance database.

Keywords— **Sensor network, Security, Provenance, Bloom Filtering**

I. INTRODUCTION

WIRELESS sensor networks are most increasingly used in several applications such as wild habitat monitoring, forest fire detection, and military surveillance area. After being deployed in the field of interest, sensor nodes organize themselves into a multihop network area with the base station. Typically, a sensor node is severely constrained in terms of computation capability and energy reserves. Sensor networks are used in numerous application domains,such as cyberphysical infrastructure systems, environmental monitoring and power grids. Data are produced at a large number of sensor node sources and processed in network at intermediate hops network on their way to a Base Station that

performs decision-making. The diversity of data sources create the need to assure the trustworthiness of data such as only trustworthy information is considered in the decision process. In a multi-hops sensor network and data provenance allows the BS to trace the source and forwarding path of an individual data packets. Provenance must be recorded for each packet, but important challenges arise due to the tight storage, energy and bandwidth constraint of sensor nodes. Therefore, it is necessary to devise a light-weight provenance solution with low overhead. Hence it's necessary to address security requirements like confidentiality, integrity and freshness of provenance. Our important goal is to design a provenance encoding and decoding method that satisfies security and performance need. 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 Base station extract and verifies the provenance information. We also devise an extension of the provenance encoding scheme that allows the Base station to detect if a packet drop attack was staged by a malicious node.

Section II describe background and Section III describes the system architecture of the proposed system. The details of secure provenance encoding and decoding is given in Section IV implementation and related work in Section V.

II. 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 anattacker 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.

III. SYSTEM ARCHITECTURE

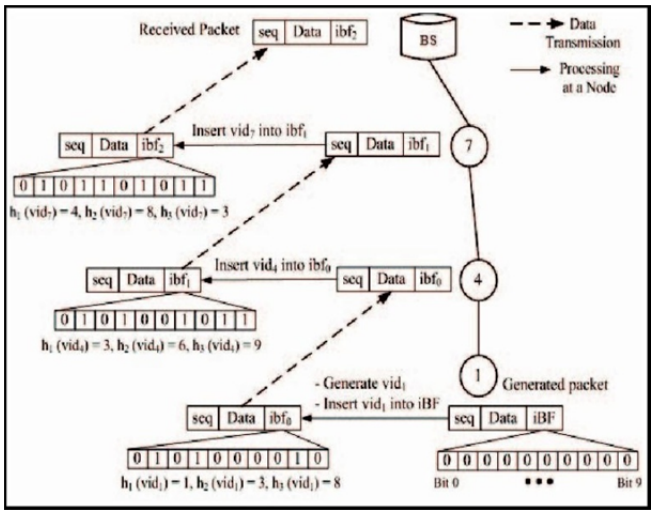

Figure1: Mechanism for encoding provenance (node 1 is data source).

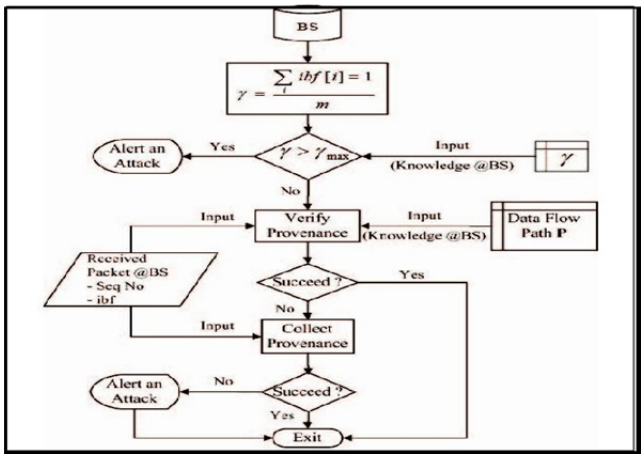

Figure2: Provenance processing workflow at the BS upon receiving a packet.

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 (in-packet 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.

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 security for data provenance and data-provenance binding.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 in-packet Bloom filter (iBF). 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 Base station. We 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.

B. Provenance Encoding

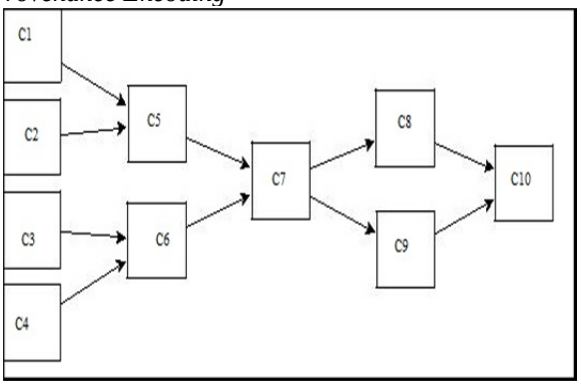

Figure3: Provenance graph

The Figure shows that to produce the final result, the contributor C5 uses the outputs of contributors C1 and C2 while 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-justified.

C. 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.

Algorithm-1 Provenance Verification:

Input: Received packet with sequence seq and iBF ibf.
Set of hash functions H, Data path P = < n l 1 , ..., n 1 , ..., n p >
BF c ← 0 // Initialize Bloom Filter
for each n i ∈ P do
vid i = generateVID (n i , seq)
insert vid i into BF c using hash functions in H
endfor
if (BF c = ibf) then
return true // Provenance is verified
endif
return false

Algorithm-2 Provenance Collection:

Input: Received packet with sequence seq and iBF ibf. N Set of nodes (N) in the network, Set of hash functions H

1. Initialize
Set of Possible Nodes S ← ∅
Bloom Filter BF c ← 0 // To represent S
2. Determine possible nodes in the path and build the representative BF
for each node n i ∈ N do
vid i = generateVID (n i , seq)
if (vid i is in ibf) then
S ← S ∪ n i
insert vid i into BF c using hash functions in H
endif
endfor
3. Verify BF c with the received iBF
if (BF c = ibf) then
return S // Provenance has been determined correctly
else
return NULL // Indicates an in-transit attack
endif

D. DETECTING PACKET DROP ATTACKS

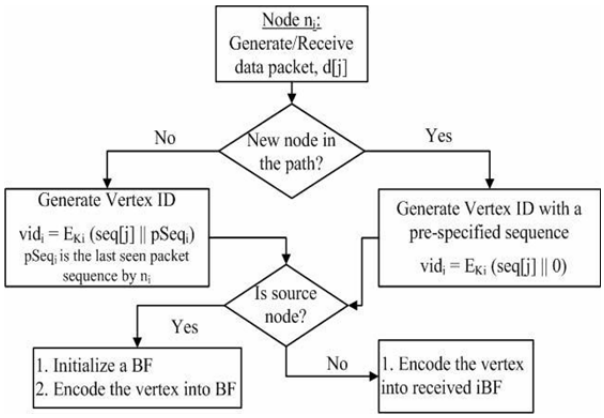

Figure 4: Extended provenance framework to detect packet drop attacks and identify malicious nodes.

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.

V. 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.

VI. 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 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 prove that the proposed scheme is effective and scalable. In future work, we plan to implement a real system prototype of our

REFERENCES

[1] Salmin Sultana,Gabriel Ghinita, and Mohamed Shehab, *Member*" A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks" *Member, IEEE,* Elisa Bertino, *Fellow, IEEE, , IEEE* [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] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A virtual data system use for representing, querying" in Proc. of the Conf. on Scientific and Statistical Database Management, 2002, pp. 37–46.

[3] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance aware storage systems," 2006, pp. 4–4.

[4] W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. Loo, and M. Sherr, "Secure network provenance," in Proc. of ACM SOSP, 2011, pp. 295–310.

[5] A. Syalim, T. Nishide, and K. Sakurai, "Preserving integrity and confidentiality of a DAC model of provenance," in Proc. of the Working Conf. on Data and Applications Security and Privacy, 2010, pp. 311–318.

[6] B. Yu, S. Kallurkar, "A demspter shafer approach to provenance awareness trust assessment," in CTS 2008: International Sym-posium on Collaborative Tech. and System, pp. 383–390, May 2008.

[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