A Light Weight Secure Provenance Scheme in Detecting Forgery and Packet Drop Attack in WSN

Bhanushree P S
(Student)
Department of Computer Science & Engineering
Don Bosco Institute of Technology
Bangalore, Karnataka

Manoj H M
(Assistant Professor)
Department of Computer Science & Engineering
Don Bosco Institute of Technology
Bangalore, Karnataka

***Abstract*— Wireless Sensor Network is widely used in many application domains. The nodes in Wireless sensor networks collect data from many sensor nodes is passes through the intermediate node and then can be aggregated at single node. This collected data is used for decision making in critical applications. The security, integrity and confidentiality of the transmitted data are the most important part in the WSN transmission. There are many possible attacks like provenance forgery, Packet drop attack, DOS attack, Jamming attack etc. are found in the WSN while transmitting the data. Data provenance keeps log information of data about who accessed this data, who modified this data, the path from the data is traversed etc. Data provenance has important role in the evaluation of trustworthiness of data therefore, it is important to secure data provenance. This paper proposes a secure provenance scheme to overcome the Packet Drop attack and forgery Attack.**

Keywords—Wireless Sensor Networks (WSN), Provenance, Forgery, Packet Drop, DOS, InPacket Bloom Filter.

I. INTRODUCTION

Wireless 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.. Security is one of the main characteristic of wireless sensor network affected with any attacks. Provenance, a mechanism of trust and reputation evaluation is an indispensable component to enhance the security of the entire network. Since provenance records the history of data acquisition and transmission, it is consideration as an effective mechanism to evaluate the trustworthiness and security of the data. It also provides the information about the operations performed on data. Reducing the size of the provenance is crucial in WSN as it is composed of a large

Number of sensor nodes. The limitation of provenance in WSN is tight storage, limited energy and increased bandwidth consumption of the sensor node. Furthermore sensors often operate in an untrusted environment, where they may be subject to attacks. Provenance function is also deals with the detecting malicious node in network and to detect the packet drop in network. Provenance trustworthiness is very important in large scale sensor network as it is deployed in a military information network and trust assessment is a crucial task. In the computational world, as all kinds of information can easily be changed, provenance becomes an important way of keeping track of alteration. 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.

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.

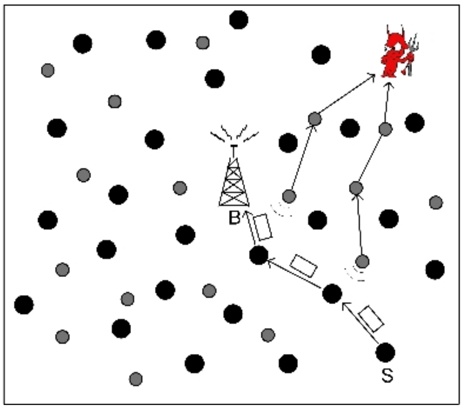

Fig. 1. Attack in Wireless Sensor Networks

II. RELATED STUDY

Ramachandran [1] proposed Pedigree provenance scheme in which each packet is tagged with provenance data. Tagger is deployed at each host which tags each packet with provenance data. Paper [1] used provenance data for traffic classification and Arbiter is deployed at each host which decides what to do with received packets having specific tags. Packet classification before Pedigree is mainly dependent on the IP addresses and port numbers but, after pedigree it has used tag information on the tags for packet classification. Pedigree scheme does not consider adversary network case and hence cannot deal with forgery attacks in the WSN.

Paper [2] addressed that network accountability and failure analysis is important for network management. It also described the need of network provenance. Paper [2] proposed ExSPAN provenance system in distributed environment. ExSPAN used data provenance to prove the state of the network. ExSPAN was developed using rapid net which is based on ns3 toolkit. Experimental results showed that the system is generic and extensible. Same as Pedigree [1] this scheme also did not consider security of the provenance data.

Wenchao Zhou [3] et.al observed the need of securing the provenance information and proposed a scheme named, Secure Network provenance which gives proof for the state of the provenance data. Network operator can detect faulty nodes and also can assess the damage to network from such faulty nodes. Snoopy named SNP is proposed in paper and experimental results showed that Snoopy can prove state of provenance data in malicious WSN model.

SNP scheme did not consider the limitations of WSN i.e. limited bandwidth, low battery and low memory. Paper [4] addressed the need to find source of the data which is transferred over the internet and proposed a scheme which provides strong integrity and confidentiality of provenance data. Proposed scheme is designed in such way that it can be deployed at application layer Experiments showed that providing the integrity and confidentiality to the provenance data results into overload with range 1% to 13%. Proposed approach gives control over the visibility of provenance data and assures no one can modify the provenance data without detection.

Integrity and confidentiality is achieved through encryption and incremental chained signature mechanism. Paper [5] proposed a method to secure directed acyclic graph of the provenance data. Proposed method used digital signature in which provenance owner and processors tags or signs nodes. The relationship between provenance data graph and integrity is validated by checking the signatures. Both paper [4] and [5] are generic solutions which can be applied to any network and they are not designed with consideration of the nature of WSN. Paper [6] proposed a mechanism in which sensor data is tagged with its provenance data automatically and provenance data can be recovered from this tagged data.

Experiments with different scenarios proved robustness of this scheme. Special feature of this scheme is that, the provenance data is embedded into actual sensor data. Proposed system does not provide any way to provide security to provenance data. Paper [7] focused on provenance management and proposed a novel secure provenance transmission scheme in which provenance is embedded into inter packet timing

domain and paper also considered limitations, requirements of WSN. Proposed scheme is different from traditional watermarking schemes. Provenance information is recovered using optimal threshold bases mechanism to reduce the provenance recovery errors. Proposed scheme is based on the spread spectrum watermarking technique and it is efficient against various sensor network or flow watermarking attacks. This scheme assumes that provenance data remains same for flow of the packets Paper [8] described the design of the bloom filter data structure and its efficiency. Bloom filter is vector of n bits. When data is encoded into bloom filter, set of hash functions is used. Data to be encoded is hashed using hash function. Output of the hash function will be integer values. Initially bit vector contains all bit value equal to 0 bit. At output, integer index is set to 1. Main purpose of bloom filter is to check the membership of element i.e. once element is encoded; membership of the data can be checked. Paper [8] discussed the potential network applications of bloom filter data structure and described suitability of the bloom filter for network applications.

Paper [9] focuses on security of the provenance data specific to wireless sensor network. Paper proposed a scheme to detect forgery on provenance data, detection of packet drop attack and also identifies the attacker of the packet drop attack. Proposed scheme used packet bloom filter data structure for encoding provenance data. 3 hash functions are used to encode the provenance data in packet bloom filter. Uses of bloom filter data structure results into lightweight scheme which is suitable to wireless sensor

network. Each packet consists of sequence id of the packet, actual sensor data and n-bit bloom filter vector. To detect the forgery attack, ID of the each node in path is encoded into bloom filter vector. It is assumed that base station knows the path of the received packet. When packet is reached at the base station in the WSN, fresh bloom filter is taken and encoded with all nodes in the path. If generated bloom filter and bloom filter extracted from received packet are same then there is no forgery attack else there is forgery attack. Actual sensor data is also secured along with provenance data with proposed scheme in this paper. Experiment results proved the effectiveness and the lightweight nature of the scheme

III. SYSTEM DESIGN

The Major aim of this paper is to design an energy-efficient secure provenance mechanism scheme. The Proposed Scheme consists of the following models.

A. Network Model

We have created a multi hop 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 of nodes n i and n j that are communicating directly with each other. The Base station assigns each node a unique identifier node ID and a symmetric cryptographic key Ki.

B. Data Model

We consider a multiple-round process of collecting data. Each sensor generates data periodically, and individual values are aggregated 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.

IV. PROPOSED ARCHITECTURE

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 designs 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 propose provenance encoding scheme and data packet loss detection mechanism.

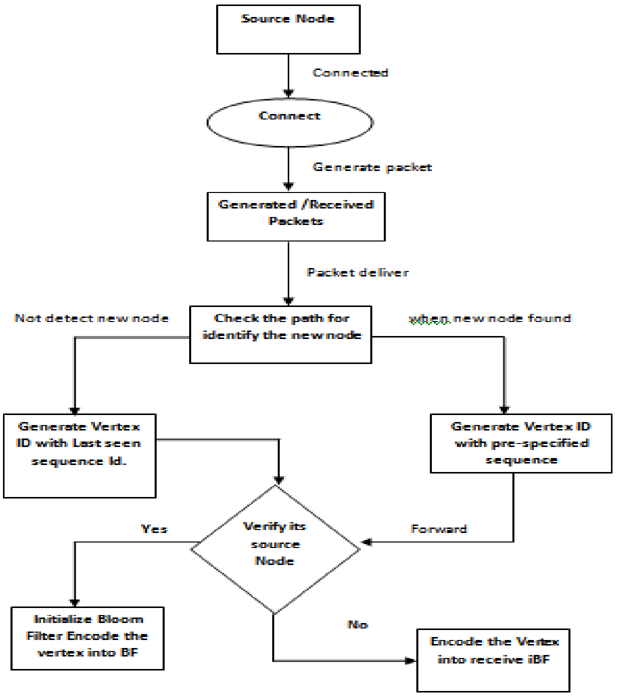
Source Node
Connected
Connect
Generate packet
Generated /Received Packets
Packet deliver
Not detect new node
Check the path for identify the new node
when new node found
Generate Vertex ID with Last seen sequence Id.
Generate Vertex ID with pre-specified sequence
Yes
Verify its source Node
Forward
Initialize Bloom Filter Encode the vertex into BF
No
Encode the Vertex into receive iBF

Fig. 2. Flowchart Representing Provenance Processing

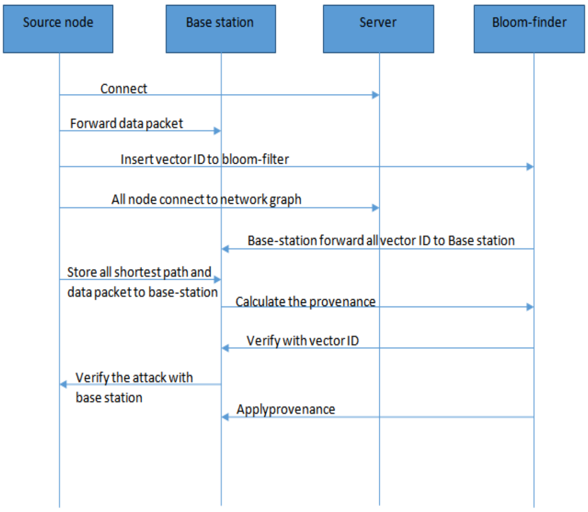
Source node
Base station
Server
Bloom-finder
Connect
Forward data packet
Insert vector ID to bloom-filter
All node connect to network graph
Base-station forward all vector ID to Base station
Store all shortest path and data packet to base-station
Calculate the provenance
Verify with vector ID
Verify the attack with base station
Applyprovenance

Fig. 3. Sequence of Operation of In Packet Bloom Filter

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.

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
```

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. PERFORMANCE EVALUATION

We implemented and tested the proposed techniques We consider a network of 100 nodes and vary the network diameter from 2 to 14. All results are averaged over 100 runs. First, we look at how effective the secure provenance encoding scheme) is in detecting provenance forgery and path changes. Next, we investigate the accuracy of the proposed method for detecting packet loss. Finally, we measure the energy consumption overhead of securing provenance.

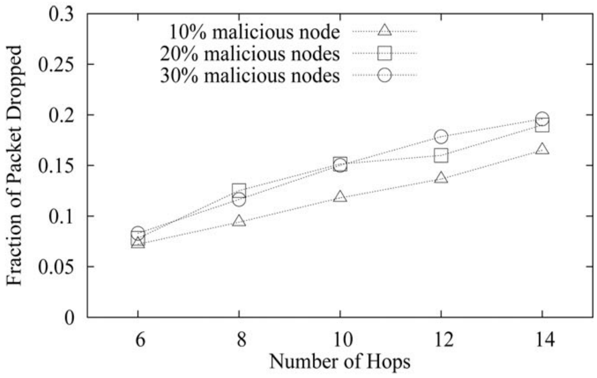

Fig. 4. End-to-End Packet Drop

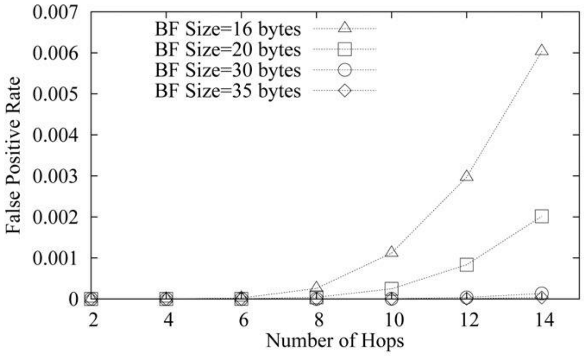

Fig. 5. Packet Drop Detection Rate

VI. CONCLUSION

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 incorporate 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.

REFERENCES

[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] S. Sultana, E. Bertino, and M. Shehab, “A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks,” in Proc. of ICDCS Workshops, 2011, pp. 332–338.

[3] L. Fan, P. Cao, J. Almeida, and A. Z. Broder, “Summary cache: a scalable wide-area web cache sharing protocol,” IEEE/ACM Trans. Netw., vol. 8, no. 3, pp. 281–293, Jun. 2000.

[4] Kirsch and M. Mitzenmacher, “Distance-sensitive bloom filters,” in Proc. of the Workshop on Algorithm Engineering and Experiments, 2006, pp. 41–50.

[5] Rothenberg, C. Macapuna, M. Magalhaes, F. Verdi, and A. Wiesmaier, “In-packet bloom filters: Design and networking applications,” Computer Networks, vol. 55, no. 6, pp. 1364 –1378, 2011.

[6] S. Roy, M. Conti, S. Setia, and S. Jajodia, “Secure data aggregation in wireless sensor networks,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 1040–1052, 2012.

[7] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, “Chimera: A virtual data system for representing, querying, and automating data derivation,” in Proc. of the Conf. on Scientific and Statistical Database Management, 2002, pp. 37–46.

[8] 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.

[9] Y. Simmhan, B. Plale, and D. Gannon, “A survey of data provenance in e-science,” SIGMOD Record, vol. 34, pp. 31–36, 2005.

[10] R. Hasan, R. Sion, and M. Winslett, “The case of the fake picasso: Preventing history forgery with secure provenance,” in Proc. Of FAST, 2009, pp. 1–14.

[11] 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.

[12] K. Dasgupta, K. Kalpakis, and P. Namjoshi, “An efficient clustering based heuristic for data gathering and aggregation in sensor networks,” in Proc. of Wireless Communications and Networking Conference, 2003, pp. 1948–1953.

[13] A. Kirsch and M. Mitzenmacher, “Distance-sensitive bloom filters,” in Proc. of the Workshop on Algorithm Engineering and Experiments, 2006, pp. 41–50.

[14] C. Rothenberg, C. Macapuna, M. Magalhaes, F. Verdi, and A. Wiesmaier, “In-packet bloom filters: Design and networking applications,” Computer Networks, vol. 55, no. 6, pp. 1364 – 1378, 2011.

[15] S. Roy, M. Conti, S. Setia, and S. Jajodia, “Secure data aggregation in wireless sensor networks,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 1040–1052, 2012.