ISSN 2395-1621

A Dictionary Based Secure Provenance Compression For Wireless Sensor Network (WSN) Part-1

[#1]Mr.Ajit M. Karanjkar, [#2]Prof. D.H. Kulkarni

[#1]Department of Computer Engineer,
SMT. Kashibai Navale College of Engineering, Pune, India
[#2]Professor, Department of Computer Engineer,
SMT. Kashibai Navale College of Engineering, Pune, India

ABSTRACT

Dictionary based secure data in sensor networks is processed by the multiple agents; data provenance compression plays an important role for assuring data trustworthiness. Dictionary based Secure they are due to energy and bandwidth limitations of Wireless Sensor Network, it is crucial that data provenance for these networks be as compress as possible. In this approach, each sensor node in the network stores a packet path dictionary. With the support of this dictionary, there are path index instead of the path itself is enclosed with each packet. Also introduce a congestion control mechanism. So the total time to be taken to travelled from sink to base station is reduced. Trustworthiness of sensor data is also assured through an AM-FM sketch, it can defend against most of the known provenance attacks. Introduce the major objective of data aggregation is to bring together and aggregate data in an energy efficient way so that network lifetime is enhanced. it can defend against most of the known provenance attacks.

Index Terms: Provenance, dictionary based compression, sensor network, Aggregation Nodes.

ARTICLE INFO

Article History

Received: 28th January 2018

Received in revised form :

28th January 2018

Accepted: 31st January 2018

Published online :

1st February 2018

I. INTRODUCTION

Wireless sensor network have a variety of applications like environmental monitoring, building monitoring, health monitoring, military surveillance and target tracking and the data they collect are used in decision-making for critical infrastructures.

Wireless sensor network is a resource restraint if we consider energy, computation, memory and limited communication capabilities. Provenance helps gather, share and store the information which may lead to privacy and security concern in wireless sensor network. Security is one of the main characteristic of wireless sensor network affected with any attacks.

Chandela wang(2016) proposed a dictionary based secure provenance scheme which is lossless approach. In this method, each sensor node in the network stores a packet path dictionary. Which contain database of the provenance information as path indexes instead of the path itself in the provenance. This indexes are stored in a dictionary. With the support of this dictionary, a fixed size path index can be used to represent a path of arbitrary length.

Wireless sensor network present more sensor nodes need a smaller amount power for processing the sensor data since compared to broad casting to data.

Our specific contributions are:

- We formulate the difficulty of secure provenance transmission in sensor networks, and identify the challenges specific to this context.
- We design efficient techniques for provenance decoding and verification at the base station;
- We perform a detailed security analysis and performance evaluation of the proposed technique.

Dictionary Based sensor network to reduce the provenance size for large-scale wireless Sensor network. use lossy compression technique. Proposed technique compresses the packets path and represents the using distinct indexes. Secure provenance the indexes are stored in dictionary. In this paper, we propose a dictionary based secure provenance and compressing the data and lightweight scheme to securely transmit provenance for sensor data through an AM-FM sketch.

We propose a provenance encoding strategy whereby each node on the path of a data packet securely embeds provenance information within a dictionary compression, that is transmitted along with the data. Upon receiving the data, the base station extracts and verifies the provenance.

This paper we have present the data aggregation method is to select a subset of sensor nodes in the network to be accountable for fusing the sensing data from other sensor nodes to decrease the amount of data transmission.

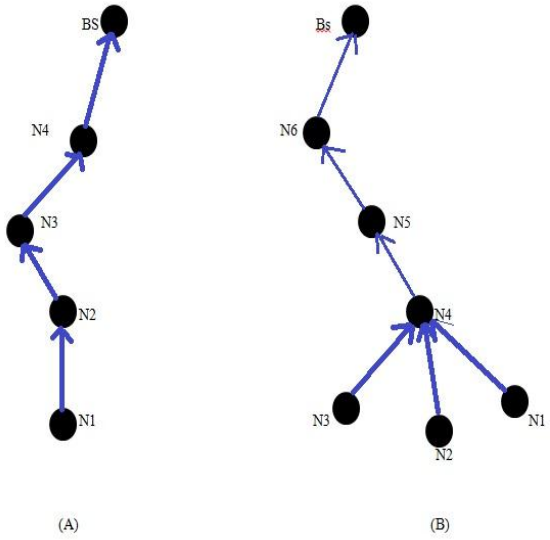

Figure 1. Provenance graph for a sensor network.

Provenance of the data item each consisting of node that manipulate or forward that item. Provenance is useful to asses trustworthiness of data. The provenance of collection of a data items representing the same event is the tree rooted at the base station.

The rest of the paper is organized as follows: section II is motivation of secure provenance for sensor Network. Section-III Review of literature secure provenance sensor network. Section IV introduces to the Proposed system. Section V explain the Existing system. Section VI Objectives of the sensor Network. Section VII introduces the System model. Section VIII describes the provenance encoding ,binding , decoding algorithm. Section IX concludes the paper.

II. MOTIVATION

Distributed system which evaluates the trust in the network that is more flexible and more responsive, which enhance the network trust in network.

There are numerous techniques and method proposed for confidentiality, integrity, and trustworthy of secure provenance transmission in WSN.

There are numerous techniques and method proposed for confidentiality, integrity, and trustworthy of secure provenance transmission in WSN. The feasibility of the asymmetric key management has been shown in Wireless Sensor Networks recently, which compensates the shortage from applying the symmetric key management for security.

Existing provenance schemes developed for conventional wired networks cannot be applied to WSNs without being modified due to both the resource-tightened nature of WSNs and the rapid provenance size increase.

III. LITERATURE SURVEY

The Author S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, A lightweight secure scheme for detecting provenance forgery and packet drop attacks in wireless sensor networks.

In this paper data are produced at a large number of sensor node sources and processed in network.

The Author Shebaro, S. Sultana, S. R. Gopavaram, and E. Bertino, A Survey On Demonstrating a lightweight data provenance for sensor networks.

In this paper develop a light weight scheme for securely transmitting provenance for sensor network.

The Author S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, A lightweight secure provenance scheme for wireless sensor networks.

In this article Lightweight provenance encoding and decoding scheme based on bloom filters.

The Author W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. T. Loo, and M. Sherr, A Survey On Secure network provenance.

In this paper is Evaluated a SNooPy prototype with three different example applications: the Quagga BGP

daemon, a declarative implementation of Chord, and Hadoop Map Reduce.

The Author S. M. I. Alam and S. Fahmy, Energy-efficient provenance transmission in large-scale wireless sensor networks.

In this paper we adapt the probabilities packet marketing (PPM) approach trace back. Further two encoding methods and combine to deal with topological changes in the network.

IV. PROPOSED SYSTEM

In order to address the drawbacks of lossy compression techniques and to address the limitation of entropy lower bound, a dictionary based approach is proposed to encode the sensor data provenance. Proposed technique compresses the packets' paths and represents those using distinct indexes. This indexes are stored in a dictionary. With the support of this dictionary, a fixed size path index can be used to represent a path of arbitrary length. This indexes are stored in a dictionary.

The use of dictionary based method allows one to keep the size of a compressed path smaller than the path's entropy at the cost of additional storage space for dictionaries. Efficient, and distributed data algorithm for encoding the provenance information as well as a centralized approach for its decoding. A secure packet sequence number generation mechanism is introduced and use the AM-FM sketch technique to secure the provenance.

V. EXISTING SYSTEM

A secure packet sequence number generation mechanism is introduced and use the AM-FM sketch technique to secure the provenance. Some provenance schemes only record the data processing or routing nodes, but discard the order in which they are traversed by the network packets.
The trustworthiness of the provenance must be assured. To reduce the provenance size for large-scale WSNs, earlier approaches use lossy compression techniques.
Some provenance schemes only record the data processing or routing nodes, but discard the order in which they are traversed by the network packets.

VI. OBJECTIVES

- Each sensor node in the network stores a packet path.
- The goal of the proposed dictionary based secure Provenance for WSNs is to guarantee a secure and efficient data transmission between two nodes.
- The trustworthiness of the provenance.
- Increase accuracy and reliability.
- Increase the lifetime of the sensor node and reduces the energy consumption.
- Data security.
- The major objective of data aggregation is to bring together and aggregate data in an energy efficient way so that network lifetime is enhanced.

Transmission of data in efficient and secure way. Proposed a dictionary based provenance scheme which is the most compact and lossless scheme up to date.

VII. PROPOSED WORK

7.1 System Model:

In this paper we have introduce and present the network model, data model, provenance model and adversary model by in System model.
Fig 2 Show block diagram of dictionary based sensor network. This diagram the source is send file to destination , that time they are first create node in dictionary based sensor network . when node is created then transfer file form source to destination .After that aggregation node is deliver the file from source to destination, and destination is receive the file from aggregation node. Suppose attacker attack in the node then file is not transfer then node is select the another path we have to use shortest path algorithm in sensor network ,and send to the file from source to destination.

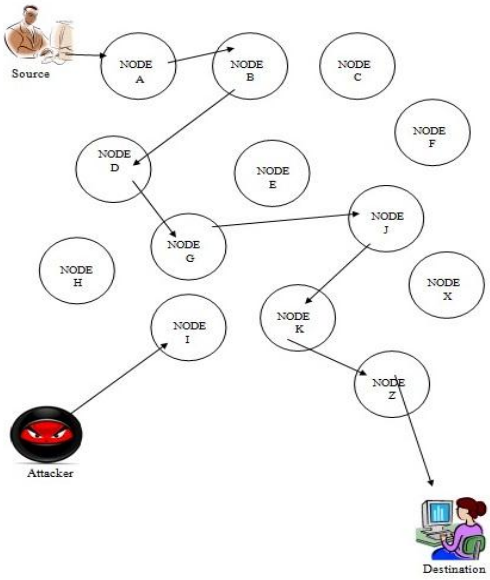

Fig: 2. Block diagram Dictionary Based Secure Provenance Compression for WSN

Types of System Model
i)Network Model.
ii)Data Model.
iii)Provenance Model.
iv)Adversary Model.

7.1.1 Network Model

The network model we consider in this paper is that of a multi-hop WSN, consisting of a number of nodes and a BS that collects data from the nodes by rounds. A round is a time interval, in which the sensors attached to the nodes generate data and then transmit the data to the BS.
Every node, except the BS, has three possible roles: data source , data forwarder and data aggregator . A data source acquires data through the sensors connected to the node and then sends the data in the form of a packet. A data forwarder relays the received packet toward the BS. A data aggregator aggregates two or more smaller packets into a new large packet and then sends the new packet toward the BS.

Nowadays, most WSN transmission protocols support packet aggregation. Any node can be a data aggregator when the aggregation conditions hold during packet transmission .
The network model of a WSN is an acyclic directed graph G(N,E), where $N = \{ni|, 1 \leq i \leq |N|\}$ is the set of node, and $E=\{eij|1 \leq i,j \leq |N|\}$the set of directed edges between nodes. $|N|$ denotes the cardinality of set N and e_{ij} denotes the directed edge from n_i to n_j.

7.1.2 Data Model

Dictionary based provenance data model we assume a multiple-round process of data collection. Each sensor node generates data periodically, and individual values are routed and aggregated towards the BS using any existing hierarchical (i.e., tree-based) dissemination scheme, e.g., Data path of p hops is represented as $< n_l, n_1, n_2, ..., n_p >$, where n1(Node 1) node representing the data source, and node n_i is i hops away from n_l.
Each data packet contains :

(i) a unique packet sequence number.
(ii) a data value, and
(iii) provenance.

The sequence number is attached to the packet by the data source, and all nodes use the same sequence number for a given round . The sequence number integrity is ensured through message authentication codes (MAC)

7.1.3 Provenance Model:

We consider *node-level* provenance, which encodes the nodes that are involved at each step of data processing. This representation has been used in previous research for trust management and for detecting selective forwarding attacks. Given a data packet d, its provenance is modeled as a directed acyclic graph $(V,)$ where each vertex $v \in V$ is attributed to a specific node $HO(v) = n$ and represents the provenance record (i.e. nodeID) for that node.

- Dictionary index: - Dictionary index (dicIndex) is used to represent the compression of a linear path.
- Packet path index: - Assume that a packet p traverses the path {nM ;n M-1, . . . , n1} to reach the BS.
- Packet Path Dictionary: Packet path dictionary (PPD) at some node ni is a database that keeps provenance information of the packets generated, forwarded or aggregated by node.

7.1.4 Adversary Model

The security risk in wireless senor network. eavesdropping. Packet injection, Jamming, Replay, Denial Of Services. In this paper adversary model can eavesdrop the network, and it can compromise legitimate nodes and extract critical information such as keys , code or data. it may also use the node to perform the attack cooperatively.
The attacker can learn the contents of the messages in transit from or to a node. This means that the attacker can observe the network . The eavesdropping attacker results from no change in safety, no change in live ness , but network level information flow.

VIII. SYSTEM ANALYSIS

8.1 Secure Provenance Scheme:

We classify the known provenance schemes for WSNs into the following categories: Provenance Encoding, Provenance Binding, Provenance Decoding.

8.1.1 Provenance Encoding

In this paper we have introduce the provenance encoding in provenance encoding they are used by data source node , forwarder node and aggregator node this three node is used in provenance encoding.
Data source node: A data source node is ni , generates the packet p, it creates row in its own table in packet path Dictionary PPD. The data source node forward the packet the BS.
Forwarder node: packet node receives the packet from some node. In Fig. 1 b) show that a packet generated by n3 is received by node n4 and then forwarded to the next node n3.
Aggregator Node: Sensor nodes are organized into a tree hierarchy rooted at the Base Station .If aggregator node ni, simultaneously receives M packets {seqi1, seqi2,…seqiM}, it aggregate into a single packet. *seqi*. Then create a new row table in packet path

dictionary(PPD). If the received packet $seq_{i1}, seq_{i2\ldots\ldots}, seq_{iM}$ are generated aggregate node.

Algorithm 1: Provenance Encoding:

Input: (ni,seqi)
Output:*prindex=(v,pathIndex)*
ifni is a data source node **then**
prIndex:v = vi
pp = *ni*
agr = φ ;
prIndex.pathIndex= <ni , φ>
end if
if*ni* is a *forwarder node***then**
prIndex:v = vi
pp = pp (∪) *ni*
agr = φ ;
prIndex.pathIndex= <nk ,ni>
end if
if*ni* is an aggregator node **then**
prIndex:v =vi
pp =ni
agr ={ seqi1, seqi2. . . . ; *seqiM*}
prIndex:pathIndex =<nb1, ni; . . . ; nbM , ni:>
end if

8.1.2 Provenance Binding

To prevent unauthorized modifications, except for the elementary provenance schemes using MAC (message authentication code) to encode provenance, the other provenance schemes have to bind the data and the provenance through additional MACs. Consequently, if either the provenance or the data are tampered, the BS is able to detect such an unauthorized modifications.
The most common MAC approaches for assuring the integrity of data are based on cryptographic hash functions, such as MD5 and SHA-1. Assuming that we apply these MAC approaches, the binding of data generated by MD5 or SHA-1 will contribute 128 bits or 160 bits to the provenance size at each node respectively, which is very expansive for resource-tightened WSNs. The distributively computing the digital digest, the AM-FM scheme also uses a symmetric encryption based digital signature approach at each node to protect the provenance

8.1.3 Provenance Decoding

Algorithm 2: Provenance Decoding:

Input:pr Index = *(v,pathIndex*)
Output:T(*Vp,Ep*)
if the AM-FM verification fails then
drop the received packet
else
if v:agr = φ**then**
T(*Vp,Ep*) = Query*pathIndex* to PPD.
else
¥= number of ';' in*pathIndex*+1
fori = 1 to ¥ do
pathi = Query branch *i* of*pathIndex* to PPD.
end for
T(*Vp,Ep*)= (path 1;. . . ; path¥)
end if
end if

Dictionary based secure provenance is 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.
The provenance decoding is graph represented as T(*Vp,Ep*) by looking up its path-Index in the Packet Path Dictionary(PPD) of the base station. when the AM-FM verification is fails then drop the received packet. Provenance decoding node n1 is the base station in the network and it previously received the packet with sequence number seq1 is generated by node and its stored in Packet path Dictionary(PPD).

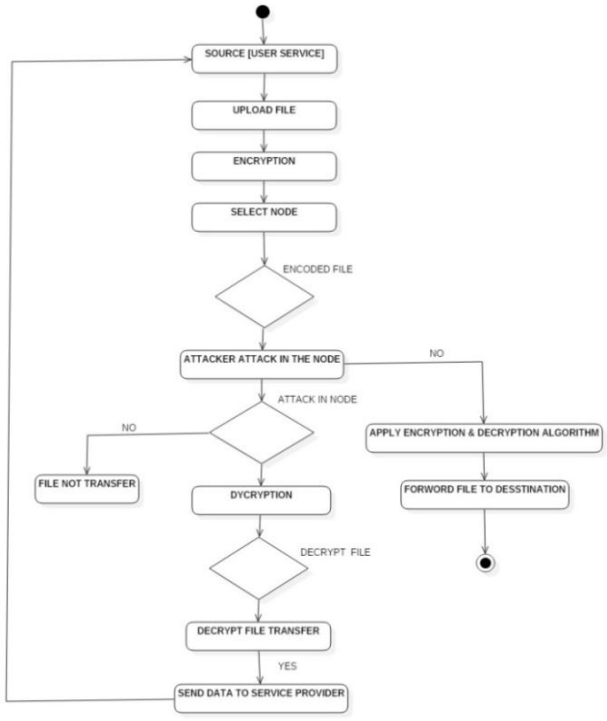

Fig:3 Activity Diagram of Proposed System.

Activity diagram we have to show how to work flow in Dictionary Based Secure Provenance Compression for wireless sensor network.
In sensor network they are source node is select and upload the browse file ,after that encryption file select path and take out IP address from destination.

The source node is multiple number of node create in sensor network and encoded file. When attacker attack in the node then file not transfer, file is decrypted and sends data to service provider. Suppose Attacker does not attack in node then apply encryption and decryption algorithm and forward file to destination.

Table 1
Dictionary of Index

Linear Path	INDEX
{n1,n2,n4, n6 ,BS}	<n1,Bs>
{n2,n4,n5,Bs}	<n2,Bs>
{n3, n4, n6}	<n3,n6>
{n4,n5,Bs}	<n4,Bs>

Provenance graph in fig.1a) and 1b) having five and fig.b seven nodes respectively. Without any compression such a provenance graph can be encoded as < n1,n2,n3,n4,BS> in fig.1a).
Path in the provenance graph in Fig1 a) is encoded as <n1,n3> and <n3,Bs>. Fig. B is multiple path are connected as branches in tree, we denote such graph is as a tree topology graph. The provenance graph can be encoded as <n1, n2, n3, n4,n5,n6,Bs>,we encode in the fig.1b) as <<n1,n4>;<n4,n5>;<n5,Bs>>These linear path and their equivalent indexes are stored in a dictionary as shown in table 1. If the graph is linear path {nx,nx-1,……,n2,n1},it can be simply represented by the index <nx,n1>

IX. CONCLUSION

In this paper we have surveyed the main approaches to secure provenance compression in WSNs. Special attention has been devoted to a systematic and comprehensive classification of the solutions proposed in the literature. In this paper we have the presented the Proposed system, existing system and objectives of dictionary based secure provenance in WSN. In this paper we have presented model data model, network model, adversary model, provenance model in dictionary based secure provenance in WSN.
Data aggregation is to bring together and to aggregate data in an energy well-organized way so that network lifetime is enhanced. Trustworthiness of sensor data is also assured through an AM-FM sketch it can defend against most of the known provenance attacks. We can control the congestion in the data aggregation process by setting out the threshold value. As to the three different kinds of provenance schemes identified in the paper, it is difficult to determine which one is always better than the others. we have presented to provenance encoding, provenance binding, and provenance decoding algorithm. In this paper we have introduced to the activity diagram of proposed system.

REFERENCES

[1]Beema K.S, Mitha Rachel Jose, "A Novel Approach of Data Compression in Wireless Sensor Networks,"IJIRCE Vol. 4, Issue 7, ISSN : 2320-9801, July 2016.

[2] S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, "A lightweight secure scheme for detecting provenance forgery and packet drop attacks in wireless sensor networks," IEEE Trans. Dependable Secure Comput., vol. PP, no. 99, p. 1, 2013.

[3] B. Shebaro, S. Sultana, S. R. Gopavaram, and E. Bertino,"Demonstrating a lightweight data provenance for sensor networks," in Proc.ACM Conf. Comput. Commun. Security, 2012,pp. 1022–1024.

[4]S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, "A lightweight secure provenance scheme for wireless sensor networks," in Proc. IEEE 18th Int. Conf. Parallel Distrib. Syst., 2012, pp. 101–108.

[5]W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. T. Loo, and M. Sherr, "Secure network provenance," in Proc. 23rd ACM Symp. Oper. Syst. Principles, 2011, pp. 295–310.

[6]S. M. I. Alam and S. Fahmy, "Energy-efficient provenance transmission in large-scale wireless sensor networks," in Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw., 2011, pp. 1–6.

[7]S. Sultana, E. Bertino, and M. Shehab, "A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks," in Proc. 31st Int. Conf. Distrib. Comput. Syst. Workshops, 2011, pp. 332–338.

[8]H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trust worthiness assessment in sensor networks," in Proc. 7th Int. Workshop Data Manage. Sensor Netw., 2010, pp. 2–7.

[9]W. Zhou, M. Sherr, T. Tao, X. Li, B. T. Loo, and Y. Mao, "Efficient querying and maintenance of network provenance at internetscale," in Proc. ACM SIGMOD Int. Conf. Manag. Data, 2010, pp. 615–626.

