Confident novel scheme for Provenance forgery and Recognition of Packet Drop attacks with Reliable Transfer of Data

Tarte Namrata[1], Supriya Nangare[2], Munmun Bhagat[3],
[1] *Student, Dept of Computer, RMDSSOE, Maharashtra, India*
[2] *Student, Dept of Computer, RMDSSOE, Maharashtra, India*
[3] *Professor, Dept of Computer,RMDSSOE, Maharashtra, India*

ABSTRACT

Abstract -The data collected from sensor networks is used in decision-making. Data are streamed from multiple sources through intermediary handling nodes that collect information. A malicious antagonist may host extra nodes in the network or change prevailing ones. Therefore, assuring high data trustworthiness is vital for correct executive. Data provenance represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces numerous challenging necessities, such as low energy and bandwidth consumption, storage efficiency and confidential transfer. In this paper, we propose a novel secure scheme to securely transmit provenance on a network. The proposed technique relies on in packet Bloom filters and AES algorithm to encode provenance and transmit confidential data. 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 and also reliable delivery of packets even if interrupted by malicious data forwarding nodes. The technique is evaluated and the results prove it to be very effective scheme that detects packet drops and also enables reliable delivery of packets.

Keyword : -

1. Computer System Organization
(a) C.2 COMPUTER COMMUNICATION NETWORKS
i. C.2.1 Network Architecture and Design
A. Wireless Communication
ii. C.2.6 Inter-networking

1. INTRODUCTION

Numerous applications require and use sensor networks. The data collected at the destination node is useful for further decisions to be made. The difference in the sources of data obtained makes reliability of data a necessity. Data provenance helps in such case where the owner and modification on data is recorded. Research showed that provenance helped where untrustworthy data was present for example SCADA systems. Although provenance management is studied since years it is not lectured properly. We examine the problem and with the help of provenance transfer detect different malicious activities. In a network data provenance helps in identifying the source and the route of the data packet at the destination node. Provenance must be recorded for each packet but there may arise problems like storage and bandwidth constraints. Hence it becomes necessary to design a security mechanism that overcomes all such constrains, as sensor networks are mostly placed in an unsecured environment. Here our goal is to design a security mechanism that satisfies all needs and meets constraints like confidentiality,

reliability and also integrity. We propose a provenance encoding strategy whereby each node on the path of a data packet securely implants provenance information within a Bloom filter that is communicated along with the data. Upon receiving the packet, the BS extracts and and the verification process is done. BS also detects whether a packet is dropped. In existing research separate channels were taken for transmission of data and provenance. Traditional systems used cryptography and other traditional mechanisms which incurred large costs. Here in dissimilarity we use Message Authentication Code(MAC) and Bloom Filters which do not vary in size and provide the required provenance information too. Bloom filters generate low error rates and also bandwidth usage is very less.

1.1 Software Requirement

Back End : MySQL DataBase
MySQL is an open-source relational database management system (RDBMS).

Front end :-
JAVA JDK 1.8.
For developing this system we will required and Eclipse IDE and implementation language will be Java.
For backend we are going to use MySQL.
Above mention software are easily available on internet. So that we can get them easily.

1.1 Hardware Requirement

1. RAM : 512 MB
2. Processor Speed : 500-800 MHZ
3. Operating System : Windows OS
4. Minimum OS version : Windows XP
5. Storage : no storage requirements as such

1.2 PROBLEM STATEMENT

To provide a novel lightweight scheme to securely transmit provenance and detect

2. SYSTEM ARCHITECTURE

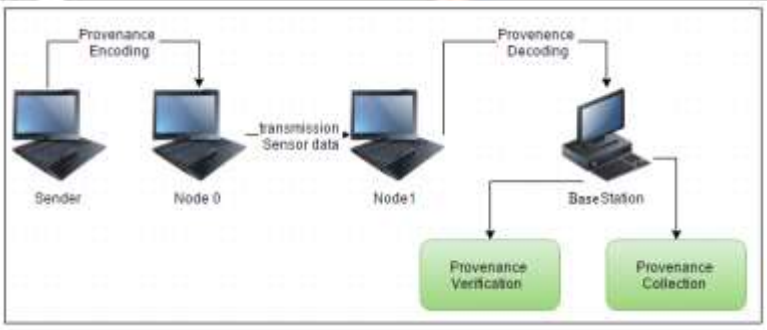


Fig. 1 System Architecture

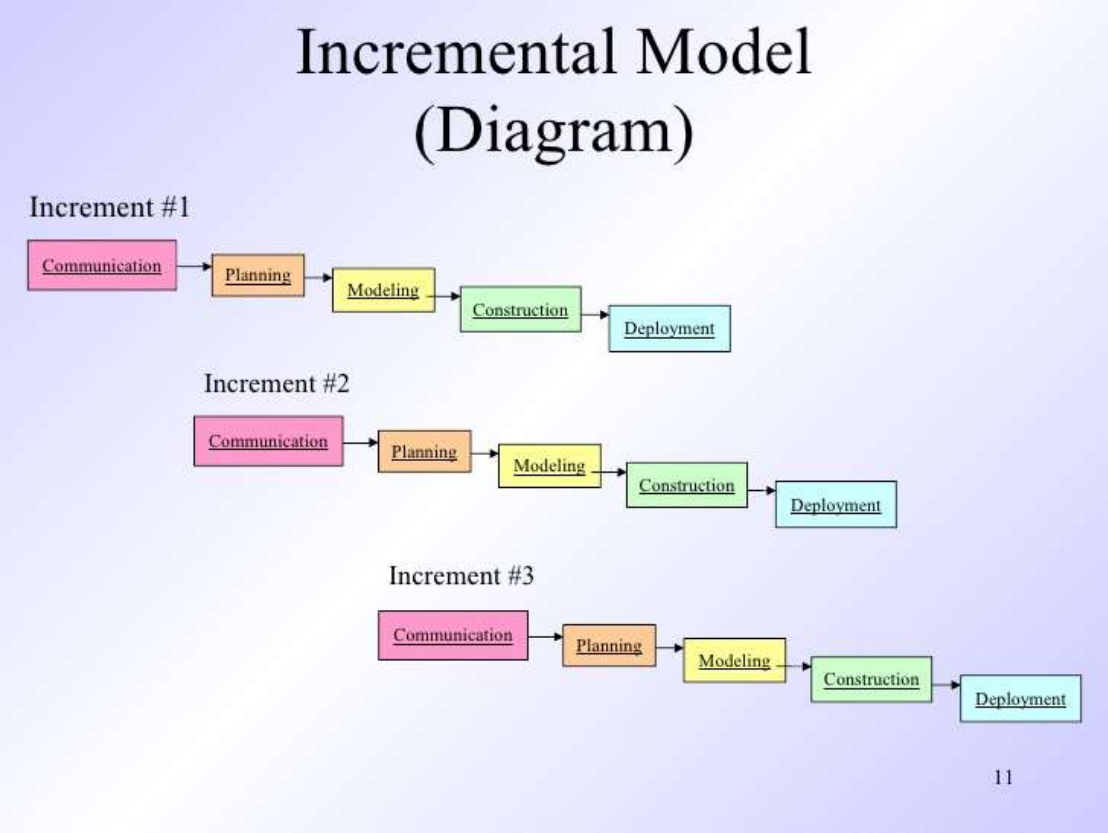
Initially user needs to register. After user registration profile of user is created. Profile is synced with the backend server. As soon as the user logs in he can transmit different files over the network to the desired nodes. These files are cut down into packets which consists of provenance information stored with the help of bloom filters. AS the file in transmitted the packet updatesthe provenance information using the bloom filters. Bloom filters give a specific unique id to very packet using some hash function. The data is transmitted over the network and if some modification is detected in the provenance info packet drop attack may me suspected. Similarly,the provenance info also keeps track of the destination where the file is to be sent hence if wrong destination receives the file the sender gets an acknowledgment for the same and the file is retransmitted to the desired location

Chart -1: System Architecture

2.1 MATHEMATICAL MODEL

- Let W be the whole system which consists:
- W= IP, PRO, OP
- IP is the input of system.
- IP= BS, G, N, L, K, H, d, ID, V, E, S, BF.
- Where,
- Let BS is the Base Station which collects data from network.
- Let G is the graph , G(N,L)
    - Where, N is the set of nodes.
    - N = ni—, 1 i —N— is the set of nodes,
    - And L is the set of links, containing an element li,jfor each pair of nodes ni and nj that are communicating directly with each other.
- K is set of symmetric cryptographic key
- H is a set of hash functions
- H = h1, h2, ..., hk .
- E is edge set consists of directed edges that connect sensor nodes.
- d is the set of data packets,
    - Let G is acyclic graph G(V,E) where each vertex v V is attributed to a specific node HOST(v) = 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.
- Identify the output as O.
    - The report generated by the function are nothing but the elements of out- put
- set.
    - Let O be the set of output parameters.
    - Let BF is the Bloom Filer, can be represented as b0, . . . , bm1.
    - Initially all m bits are set to 0.
    - To insert an element s S into a BF, s is hashed with all the k hash functions
    - producing the values hi(s) (1 i k).
- The bits corresponding to these values are then set to 1 in the bit array.
- Success Conditions: Transmission of file to desired destination
- Failure Conditions: Unable to connect to other nodes and transmit data.

2.2 INCREMENTAL MODEL



Incremental Model is one of method use for software development. In incremental model the software product is developed or build , implemented and tested in incremental order , such that time certain changes are made in the product until finished. Software product that has been developed is also maintained in this model. This model is used when the requirements keep on evolving.
The changes are also made on the basis of feedback. Incremental model follows iterative methodology.

Chart -2: Incremental Model

3. ALGORITHM TO BE USED

Here we use two algorithms namely Bloom filtering and AES algorithm for the secure transmission of data towards the destined node.

This is a data structure that is represented in the form of sets like

S={s1,s2..} using some array and hash functions. The output of each hash function hi maps an items uniformly to the range [0, m-1], i.e., an index of m-bit array. The BF can be represented as {b0, …,bm?1}. Initially all m bits are set to 0.

Let BF is the Bloom Filer, can be represented as b0, . . . , bm1.

Initially all m bits are set to 0.

To insert an element s S into a BF, s is hashed with all the k hash functions

producing the values hi(s) (1 i k).

The bits corresponding to these values are then set to 1 in the bit array.

AES i.e Advanced Encryption Standard is a symmetric block cipher used to encrypt sensitive data. Here in this case it will encrypt the provenance information and also the data packets if required.

3.1 ADVANTAGES

1. Reliability
2. Security
3. No other party can operate the data.
4.Only authorized user will receive the data.

4. CONCLUSIONS

We propose a system that detects packet drop attacks and provenance forgery along with reliable transfer of data along the path to the desired node.
If the data is received by some unwanted node it is sent to the required node using its provenance information.

5. ACKNOWLEDGEMENT

We express our sincere thanks to our Hod. Vina Lomte for her kind co-operation. We express our sincere thanks to Prof. Munmun Bhagat.

6. REFERENCES

I. 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.

II. 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.

III. 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.

IV. 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.

V. 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.