Prevention and detection of malicious attacks and prevention of provenance forgery

Munmun Bhagat[1], Tarte Namrata[2], Supriya Nangare[3]

[1] *Asst.Prof., Dept.of Comp. Engg., RMDSSOE, Maharashta, India*
[2] *Student, Dept.of Comp. Engg., RMDSSOE, Maharashta, India*
[3] *Student, Dept.of Comp. Engg., RMDSSOE, Maharashta, India*

ABSTRACT

Number of users are present in a network. Different malicious activities are performed on the data that is being transmitted over a network.The malicious attacks may delete or modify the data. they may also change the destination of the file to be sent. This system is mainly dseigned to detect such activities and prevent such files from malicious activities. The malicious activities may be of different types reporting the activities to take necessary actions is needed.

Keyword: - *Provenance, Networking, Sensor nodes*

1. Introduction

Our system works on a scheme which detects provenance forgery and packet drop attacks. The scheme is specially made in order to detect malicious activities in the network like incorrect ip address i.e. destination,modification of data and also deleting or misleading of data. The operations performed on our system are- 1)The sender that is nothing but the receiver sends the data or file. The file is then divided into packets. In our system at now we take into consideration only text files for now as they are the easiest form of a file.2) The packets are send to the client in present to the next of the server. Malicious activities could happen here.3)We demonstrate packet drop of some packets and also the data in the packets could be modified or deleted. 4)At the receiver side on checking the report of the sent fie we get the report of activities performed on the packets respectively.5)File sent to the wrong destination is also reported to the server where it takes proper actions and also resends the file.

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.

1.2 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

1.3 Problem Statement

To provide a secure and reliable transmission over network.

2. System Architecture

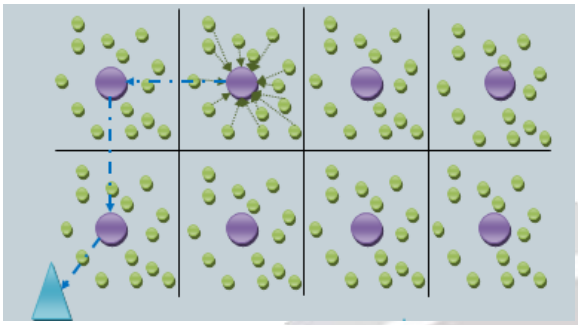

Fig.1 System Architecture

The above given architecture is for sensor networks. The different nodes present in the network collect and broadcast data to other nodes. The process of collection data is also known as Data Gathering which is denoted with the arrows.

The cluster heads hold a number of smaller nodes of similar types and store similar type of information.

Sink is also one data type where information from different clusters is collected.

2.1 Advantages

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

2.2 Drawbacks of the previous system

The previous systems need external virtual machine in order to detect suspicious system calls.

Even if number of studies have been performed on provenance nothing has been properly addressed it in sensor networks.

Detection was done but no such report was sent to the server as in our system.

Also when some packets were failed to delivered to the wrong destination they were never detected nor were they sent to the correct destination in the previous case studies.

3. CONCLUSION

In short we determine secure transmission of data from the server to the clients. Also ensuring that the malicious activities performed will be reported to the server and the server will take necessary actions. Even wrong destination

is reported and the file is resent by the server ensuring that it is sent to the correct destination making our system more reliable.

3.1 Related Work

Pedigree[3] captures provenance for network packets in the form of per packet tags that store a history of all nodes and processes that manipulated the packet. However, the scheme assumes a trusted environment which is not realistic in sensor networks. ExSPAN[4] describes the history and derivations of network state that result from the execution of a distributed protocol. This system also does not address security concerns and is specific to some network use cases. SNP [5] extends network provenance to adversarial environments. Since all of these systems are general purpose network provenance systems, they are not optimized for the resource constrained sensor networks.

4. ACKNOWLEDGEMENT

There are a number of people behind this piece of work who deserves to be both acknowledged and thanked here. We would like to thank my academic guide Prof. Munmun Bhagat and Prof. Parth Sagar, for their enthusiasm, guidance and support throughout this process. They have routinely gone beyond their duties to solve our worries, concerns, and anxieties.

6. REFERENCES

1)Salmin Sultana,Gabriel Ghinita, *Member, IEEE,* Elisa Bertino, *Fellow, IEEE,*and Mohamed Shehab, *Member, IEEE,"*A Lightweight Secure Scheme for Detecting Provenance Forger y and Packet Drop Attacks in Wireless Sensor Networks.*"*

2)Tarte Namrata,Supriya Nangare,Munmun Bhagat,"Confident novel scheme for Provenance forgery and Recognition of Packet Drop attacks with Reliable Transfer of Data",IJARIIE Volume 3 issue 1 2017

3) W. Zhou, M. Sherr, T. Tao, X. Li, B. Loo, and Y. Mao,"Efficient querying and maintenance of network provenance at internet-scale," in *Proc. of ACM SIGMOD*, 2010, pp. 615–626.

4) A. Ramachandran, K. Bhandankar, M. Tariq, and N.Feamster,"Packets with provenance," Georgia Tech,Tech.Rep.GT-CS-08-02, 2008

5) 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.