NAIRJC KNOWLEDGE IS POWER
IRJIF. I.F. : 3.821

North Asian International Research Journal of Sciences, Engineering & I.T.

ISSN: 2454-7514 Vol. 3, Issue-10 October-2017

SUPER BLOOM FILTER: IDENTIFYING TRUSTWORTHINESS OF NODES WITHIN AD-HOC NETWORKS

MAYUR BAGUL, MILIND BHAGUNDE, RASIKA GAWALI & DEEPALI BAVASKAR

Nutan Maharashtra Institute of Engineering and Technology, TalegaonDabhade,
Department of Computer Engineering, SavitribaiPhule Pune University, India

Abstract

Now a day's networking become widely used thing in the world of computer science. Where popularity of sensor networks and their many uses in critical domains such as military and healthcare make them more vulnerable to malicious attacks. In such context, trustworthiness of senor data and their provenance is critical for decision making. Lots of time a malicious node or adversary may present an extra node in network like ad-hoc network or it may compromise existing ones. In this paper we are representing an efficient and secure approach uses for transmitting provenance information about sensor data. Whatever we have developed uses super filters that are encoded as sensor data goes through various intermediate sensor nodes and they get decoded and verified at the base station. With the help of this developed technique our provenance technique will able to defend against various malicious attacks done by unknown person or node. Such as packet drop and provenance forgery.

***Keywords*: Super Bloom Filters, Provenance, Ad-hoc Networks, Security.**

INTRODUCTION

Networking is become the most popular thing in the world of computer science. Along with networking, conceptof internet is become one of the essential thing in our life.

Hence in networking networks like sensor network, ad-hoc network and so many others kind of network lots of clients and user works as a part of network to which we generally called node. In this paper we will take example of sensor network which is used in lots of different application domain like military, hospitals, vehicular sensor network and so on.

Ease of Use

In ad-hoc network with the help of data provenance we can trace the source and forwarding path of an each and every data packet. Provenance for each data packet should be get store but apart from this challenges get arise due to energy, storage and bandwidth of nodes. Therefore to give the solutions on these challenges it is essential to provide provenance solution with low overhead. We are mainly focusing on to design the mechanism of provenance encoding and decoding that can fulfill the need of security and performance.Hence solution to this problem we propose a real time provenance collection in data stream.Our project simply gives detail report on which packets are changed or drop. So this makes our project easier to use and handle.

BACKGROUND

Networking is become the most popular thing in the world of computer science. Along with networking, concept of internet is become one of the essential thing in our life. Hence in networking networks like sensor network, ad-hoc network and so many others kind of network lots of clients and user works as a part of network to which we generally called node. In this paper we will take example of sensor network which is

used in lots of different application domain like military, hospitals, vehicular sensor network and so on.

Motivation

Ad-hoc network are becoming increasingly popular in numerous application domain, such as cyber physical infrastructure system, environmental monitoring, power grids, etc. Data is produced at large no. of network nodes sources and process in network at intermediate hope on their way to the base station that perform decision making. The diversity of data sources *creates the need to assure the trustworthiness of data such that only trustworthy information is considered in the decision process. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data.*

3. System Architecture

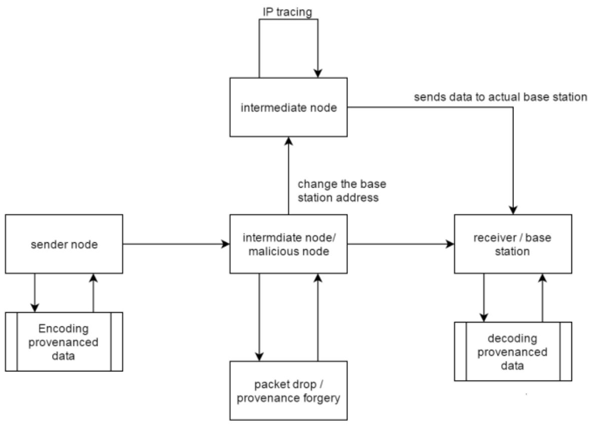

IP tracing
intermediate node
sends data to actual base station
change the base station address
sender node
intermdiate node/ malicious node
receiver / base station
Encoding provenanced data
packet drop / provenance forgery
decoding provenanced data

Fig. : System Architecture

The proposed system is most effective and secure. This proposed system actually uses client server architecture which includes single central server and so many clients which uses the smart meter. When user gets logged in or performs any

other operation that information gets stored in database. After receiving meter reading, reading is stored in database for further task. This system is all about request and response architecture.

Design of system

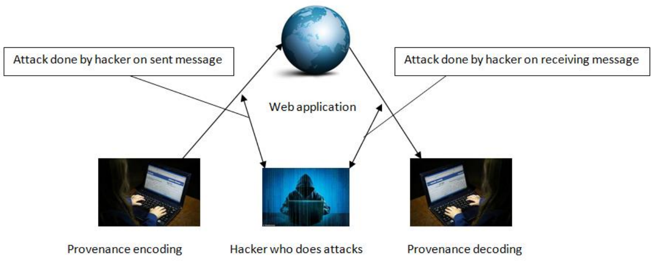

Attack done by hacker on sent message
Attack done by hacker on receiving message
Web application
Provenance encoding
Hacker who does attacks
Provenance decoding

Figure2. Design of system

When sender will send message to the destination IP at that time provenance encoding will get done with help of provenance model which will done encryption at sender side with defined key on message. Then attacker node will do attack on message as we assumed while implementing this project. When message reaches to the receiver end with the help of Super Bloom Filter algorithm we will be able to understand about what kind of attack is happened on message by after provenance decoding is get done on destination side.

PROPOSED DESIGN

From so many years since the software's were get developed lots of vulnerabilities were get emerged without knowing of anybody even including developers. Then after increased use of Software's on computer made human understandable about its secrets which was not known at the initial stage of development of software's. According to growth of the computer organization various vulnerabilities get emerged whose benefit were taken by unauthorized user which was working anonymously having bad motive to harm organizations. The rate of hacking attacks in 2000-2010 year was the massive, because there were no such system to detect or to know about anything happened to our data or message. But now here we have designed such system which will be able to detect such attacks if any attack happens on your message.

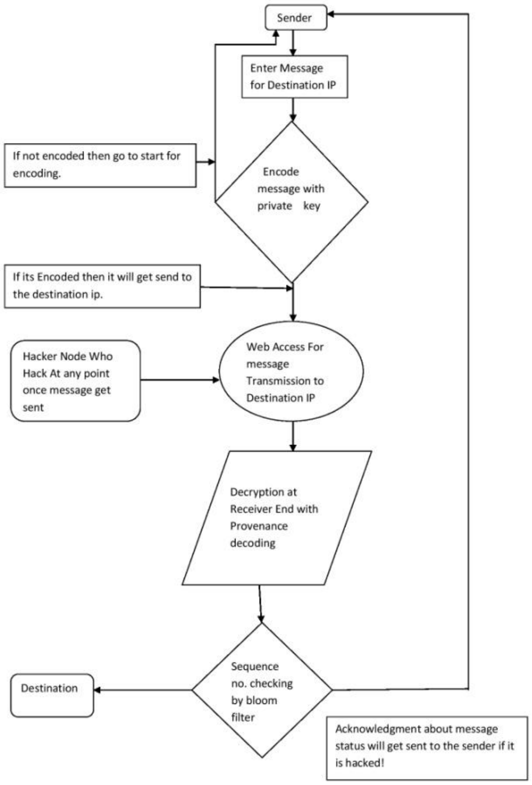
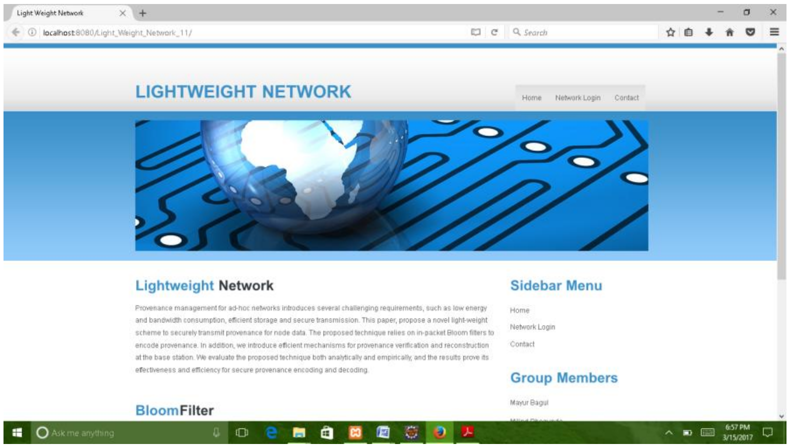

Sender
Enter Message for Destination IP
If not encoded then go to start for encoding.
Encode message with private key
If its Encoded then it will get send to the destination ip.
Hacker Node Who Hack At any point once message get sent
Web Access For message Transmission to Destination IP
Decryption at Receiver End with Provenance decoding
Sequence no. checking by bloom filter
Destination
Acknowledgment about message status will get sent to the sender if it is hacked!

Figure 3. Control flow of proposed system

Implementation



Lightweight Network

Provenance management for ad-hoc networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. This paper, propose a novel light-weight scheme to securely transmit provenance for node data. The proposed technique relies on in-packet Bloom filters to encode provenance. In addition, we introduce efficient mechanisms for provenance verification and reconstruction at the base station. We evaluate the proposed technique both analytically and empirically, and the results prove its effectiveness and efficiency for secure provenance encoding and decoding.

BloomFilter

Figure 4. Hompage of Software

In This Project we are developing source coding in Java Language along with support of Servlet coding for development of web pages to create web application as we can see which we have used for transmission of message from sender to receiver end. To enable local client we have used Tomcat apache server 8.0 with the help of which we are able to show sender to client message transmission process. For database connectivity we are using XAMP software which give support to MYSQL libraries. For this project we have done Manual Testing.

ALGORITHM

Algorithm 1

AES algorithm for encryption and decryption steps :

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (ciphertext).

Algorithm 2:

MD5

1. Pad message so its length is 448 mod 512

2. Append a 64-bit original length value to message

3. Initialize 4-word (128-bit) MD buffer (A,B,C,D)

4. Process message in 16-word (512-bit) blocks:

5. Using 4 rounds of 16 bit operations on message block bu_er

6. Add output to buffer input to form new buffer value

7. Output hash value is the final buffer value

Technology Overview

XAMPP

XAMPP is regularly updated to the latest releases of Apache, PHP and Perl. It also comes with a number of other modules including Open SSL, wordpress and more. Self-contained, multiple instances of XAMPP can exist on a single computer, and any given instance can be copied from one computer to another. XAMPP is offered in both a full and a standard version.

MySQL

MySQL is an open-source relational database management system. MySQL is a central component of the LAMP open-source web application software stack. MySQL works on many platforms. MySQL can be built and installed manually from source code, but it is more commonly installed from a binary package unless special customizations are required. Though MySQL began as a low-end alternative to more powerful proprietary databases, it has gradually evolved to support higher-scale needs as well.

Java

Java is a functional computer programming language that provides high protection of data. It is a platform independent language. It is used as object oriented language which helps to create applications in a very efficient manner. It is **Write Once Run Anywhere** type of language which reduces the task of compiling code each time it is executed on new system. It is also used for creation of web based applications or develop business applications.

Eclipse Kepler

It is an**Integrated Development Environment.** It contains a base workspace and extensible plug-in system for customizing environment. Java is mostly preferred for eclipse that can be used to develop interactive applications. It can also be used to develop packages for the software calculations.

MATHEMATICAL MODEL

1) Let W be the whole system which consists of :

W= {IP, PRO, OP}

2) IP is the input of system.

IP= {BS, G, N, L, K, H, d, ID, V, E, S, BF}.

Where, BS is the Base Station which collects data from network.

3)Let G is the graph , G(N,L)

Where, N is the set of nodes.

N = {ni|, $1 \leq i \leq |N|$} is the set of nodes,

And L is the set of links, containing an element li,j for each pair of nodes ni and nj that are communicating directly with each other.

4) K is set of symmetric cryptographic key

5)H is a set of hash functions .

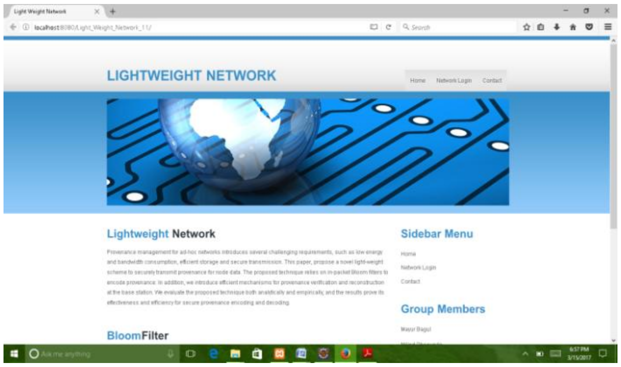
H = {h1, h2, ..., hk} .

6)E is edge set consists of directed edges that connect sensor nodes.

& d is the set of data packets.

RESULT

Home page of our Project:



Lightweight Network

Provenance management for ad-hoc networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. This paper, propose a novel light-weight scheme to securely transmit provenance for node data. The proposed technique relies on in-packet Bloom filters to encode provenance. In addition, we introduce efficient mechanisms for provenance verification and reconstruction at the base station. We evaluate the proposed technique both analytically and empirically, and the results prove its effectiveness and efficiency for secure provenance encoding and decoding.

BloomFilter

Sidebar Menu

Home

Network Login

Contact

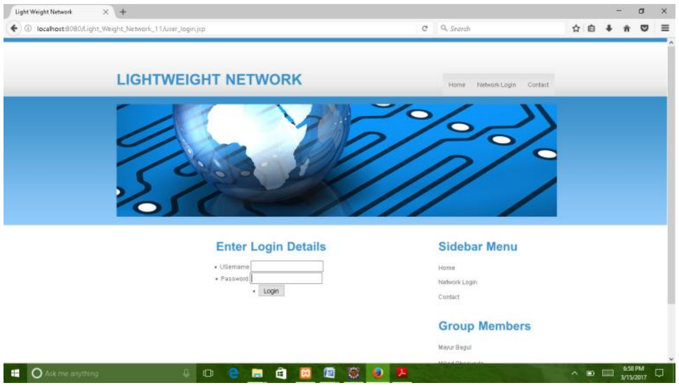
Group Members

Mayur Bagul

.

Figure. This is main home page of our project.

User login page : -



Enter Login Details

- USername
- Password
- Login

Sidebar Menu

Home

Network Login

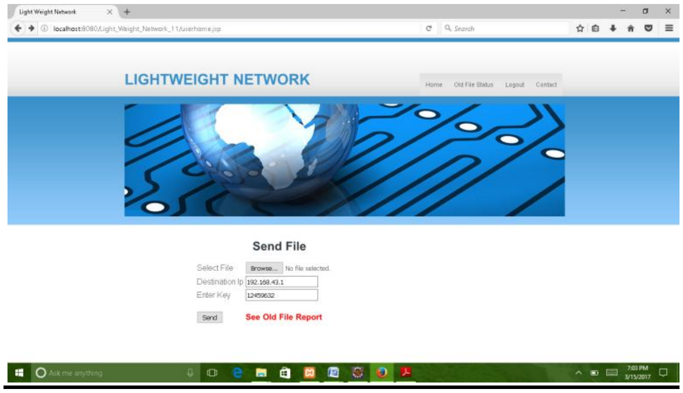
Contact

Group Members

Mayur Bagul

Figure . This is sender module first we have to login from Sender module .

Sender module :



Send File

Select File Browse... No file selected.

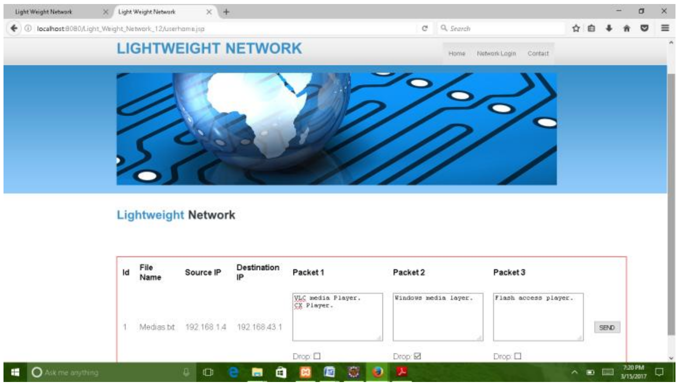
Destination Ip 192.168.43.1

Enter Key 12459632

Send See Old File Report

Figure . From this module we can send our file to required destination IP.

Attacker module.

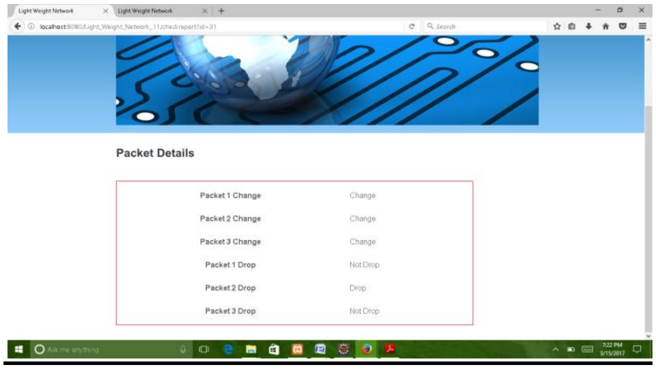


Lightweight Network

Id	File Name	Source IP	Destination IP	Packet 1	Packet 2	Packet 3	
1	Medias.txt	192.168.1.4	192.168.43.1	VLC media Player. CX Player. Drop □	Windows media layer. Drop ☑	Flash access player. Drop □	SEND

Figure. This is attacker module. From this module attacker can change Some packets also he may change some data in it.

Packet change/drop report :



Packet Details

Packet 1 Change	Change
Packet 2 Change	Change
Packet 3 Change	Change
Packet 1 Drop	Not Drop
Packet 2 Drop	Drop
Packet 3 Drop	Not Drop

Figure . Here we get detailed report about which packets are dropped or changed.

APPLICATIONS

1) Military Application

2) Healthcare System.

3) VANET etc.

CONCLUSION

In this paper we have used light-weight In-Packet Super Bloom Filters that are encoded as sensor data travels through

intermediate sensor nodes, and are decoded and verified at the base station. Our provenance technique is also able to defend against malicious attacks such as packet dropping and allows one to detect the responsible node for packet drops.

REFERENCES

[1] 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 Transactions on Dependable and

Secure Computing vol.6 , no.1, January 2016.

[2] 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.

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

[4] 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.

[5] P. Jokela, A. Zahemszky, C.E.Rothenberg, S. Arianfar, and P. Nikander, “LIPSIN: Line Speed Publish/Subscribe Inter-Networking” .

[6] A. Kirsch and M. Mitzenmacher, “Distance-sensitive Super Bloom Filters,” in *Proc. of the Workshop on Algorithm
Engineering and Experiments*, 2006, pp. 41–50.

[7] 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.

[8] 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.

[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] 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–