International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 8, ISSN No. 2455-2143, Pages 70-74
Published Online December 2017 in IJEAST (http://www.ijeast.com)

REDUCING SECURITY FEEBLENESS ISSUES IN CENTRALIZED SERVER DATA BY THE ATTACKERS USING SENSORS

Dr.R.V.S.Lalitha
Department of C.S.E
ACET, Surampalem, AP, India.

Dr.G.Jayasuma
Department of IT
JNTUK-UCEV, Vizianagaram, AP, India

Abstract: **Data security and access control plays an efficacious role in protecting centralized server to restrict unauthorized/unauthenticated users in misusing the system. The security is imperious for outsourced classified data. This paper emphasizes the issues related to protecting centralized data from access by illegal users. The proposed a novel technique uses sensor approach to protect data whenever it is trapped. Use of sensor networks in restricted places provides utmost facility in handling the problem automatically without out the intervention of manual process. The proposed solution prevents data tampering as traffic analysis is done automatically using sensors in both inter and intra cluster communication.**

Keywords: Data tampering, attacks, clustering, hidden terminal problem

I. INTRODUCTION

The data hosted on the web is accessible to all the users if no security is provided. Suppose, if the data is confidential and only allowed users are required to access, then username and password are required or some key exchange process is to be done to allow authorized users to access data and restrict others not to access. This leads to major problem because attackers find several means to break passwords and tampering of data. In this paper, novel mechanisms are proposed to detect and trace the path of illegal access. The various issues related to trapping data are discussed the possible solutions are suggested based on the type attack occurred. The solution analysis includes traffic analysis, identifying type of attacks, how to handle localization issues, adopting cluster head mechanisms. Also rules for analyzing integrity violation are discussed.

II. RELATED WORK

The unauthorized data access by various attackers is analyzed using history information and statistics collected. The network attacks are detected using monitors[1,7]. The issues are part of intrusion detection system. In the host based intrusion detection systems, the process of detection is to be refined by introducing automatic detection system. The various possible chances of occurring attacks are to be predicted and need to be tracked for taking protecting sensitive data. Physical layer attacks, data link layer attacks and network layer attacks definitely do some harm to server databases. Apart from that attack against clock synchronization and symmetric key cryptography effects security factor of the server database. The minimization of self stabilization of network is done using clustering mechanisms [2].Self-stabilizing algorithms in sensor networks helps in detection of malicious nodes and later they will re organized using clustering algorithms. This approach targeted to put limit on unreliable communication. Cluster Gateway Switch Routing Protocol(CGSR) is used to cover maximum number of nodes in the cluster. Proactive routing protocols are discussed to update routing information from node to node time to time and Reactive protocols are used to update information when the route to the destination is required[3]. Optimal rank aggregation methods and Markov chain models[12]reduces the overhead of computation while doing meta-search operations. In distributed sensor networks data is collected by individual sensors and sent to central nodes for processing as the bandwidth of sensors is very much low[6,13].

In this paper, Section 1 describes previous work related to unauthorized data access by attackers and by other means. Section 2 illustrates schematic representation accessing centralized server data accessed by various devices. In Section 3, the various means of accessing data by authorized users is illustrated. And in Section 4, proposed solutions to Feebleness issues in Centralized Server Data using Sensors are discussed. The prototype of trapping central server data using OPNET modeler is elaborated in Section 5. In conclusion, the effective usage of sensor in automatic detection of attacks is emphasized.

III. CENTRAL SERVER DATA ACCESS BY AUTHORIZED USERS

Typical approach to allow authorized users to access data from centralized server is by giving username and password whenever confidential data is to be accessed from the server .Authentication needs to be provided to the users, who are all accessing it.

Server
Various means of Authorized user access

Fig.3.1. Centralized Server data access by authorized users

During the process of accessing data, some of the authorized users may reveal the confidential information to outsiders. In Fig.3.1.the various possibilities of accessing server information using online services are shown.This problem needs to be tackled carefully. In this paper a new solution is proposed to identify the packet traversal path and the node where the data is trapped using sensors at the trapped path and trapped node.

The various possibilities of tampering data from centralized server are:-

3.1. In general when data is tampered, it is supposed to be done through routers. Routers play a predominant role in restricting users when it is not required.

3.2. Identifying the types of attacks:

Attacks are categorized into three types:

i) Physical Layer attacks: These attacks are done by jamming signals.

ii) Data Link Layer attacks: These attacks are done by modifying data during transmission.

iii) Network Layer Attacks: These attacks are done because of providing inappropriate authentication to users.

3.3. Localization issues: The problems aroused due to insecure localization techniques adapted.

3.4. Insecure clustering algorithms implemented: Various clustering techniques like Hierarchical clustering, Grid based clustering, K-Means clustering etc. helps in collecting useful information from raw data[14].

3.5. Mismanagement of Routing Protocols

3.6. Inadequate aggregation techniques at receiver end[10].

All these issues need to overcome for providing utmost security to effective communication.

IV. PROPOSED SOLUTIONS TO FEEBLENESS ISSUES IN CENTRALIZED SERVER DATA USING SENSORS

4.1. Traffic analysis at routers

The routing problems can be minimized by analyzing the data moving from key routers using sniffers eg. Ethreal, Wireshark etc. The application of Motion tracking sensors at critical positions, helps in capturing the path of packets arrived. If there is any change in routing path, these sensors provide automatic alerts. The data captured by the sensors is verified by either Ethreal or Wireshark tools.

4.2. Identifying the types of attacks

To avoid physical layer attacks, identify the jammers that cause the some of the packets to be blocked. Re transmission is required in case the missing packets are more. Use of CRC check for cross-verifying the information received; at data link layer avoids data link layer attacks. Weak authentication allows faulty users to access network. Strong authentication is to be provided in network layer. Effective authentication techniques like RSA or AES algorithms at Broadcast Receivers to broadcast data help in maintaining the integrity of data.

By Adapting micro sensors at physical, data link and network layers, provides a threat against attacks. To develop the prototype, motion sensors in Android mobiles fit the solution. The captured data is to be sent to Web Server through Google Cloud Messaging services.

4.3. Handling Localization issues

The terminals that are exposed to hidden terminal problem and near and far terminal problem are to be identified and ports that are accessible to other cells are to be blocked.
Using Mobile sensors, current Geographic positions can be tracked. Also, the data captured by the sensors can be stored in a local database for further analysis. The methods, get Latitude() and get Longitude() are used to trace the location information. This information is useful in detecting the location of data captured.

4.4. Incorporating Cluster Headmechanism

When clustering is used, all the data is to be transmitted through cluster heads. There is a possibility of bypassing the messages without using cluster heads[9]. These nodes are to be traced and take necessary action to check IP corresponding to block further transmission of messages.

Clustering is done based on the coverage area of the sensor sensing medium. As the sensors are low powered, Cluster Head mechanism helps in fast transmission. Hierarchical Clustering is the best clustering method in forming nodes into clusters. As it groups the nodes nearby and covers all the nodes that are nearer to the cluster heads. Since the sensor's transmission range is short, cluster head mechanism leads to quick transmission of messages.

4.5. Managing Routing Protocols

The header information provided in the Routing protocol must be adequate. If some of the information is missed in the header information, there will be problem in deciding whether the information is reliable or not. Object tracking using GPS over GSM networks using sensors and RFID tags make easier approaches over traditional approaches[15].In case of weak signal communication, decoding of header information leads to erroneous results at data link layer. As sensors do not require Line of Sight(LOS) communication, avoid the problem of hidden terminal problem. Also, they work well in the absence of signal.

4.6. Checking for integrity of the data received

Usually the data sent and data received at both source and destination is compared for integrity checking. Apart from that, the routing path traversed by the packets is also to be verified to address the problem of threat[11].Generally, Collection and Re-assembling of packets are done at receiver end. Sensor approach helps in tracking the path traversed by each packet automatically. In this particular method, the aggregation is done in several stages. The protocol is mentioned as below:

1. Place the sensors at various proxy servers.
   If the data is captured, share is using Bluetooth services to nearby nodes instantly.
2. While Bluetooth transmission takes place, it will be transmitted to Cluster Head also.
3. Thereafter, Cluster Head to Cluster Head mechanism takes place, to reach the central server.
4. Data is aggregated from the Cluster Heads and finally it reaches to centralized server.
5. A comparative analysis is made between the original data stored at the centralized server and the data collected by the sensors.
6. If the data modified is less, replace that fragment, or else complete data is to be retransmitted again.
7. The part of posterior analysis is with the location information obtained from the GPS, track the proxies from where data is trapped for taking remedial measures.

V. RESULTS AND DISCUSSION

The sample scenario to trap the network is illustrated inFig.5.1.

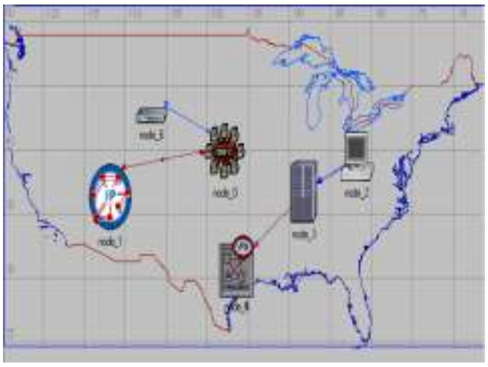

Fig.5.1. Network using OPNET IT GURU simulator to trap data from node_0 to node_3 andnode_2.

Notations used in Fig.5.1.

node_0 is the Lan using which the data can be transmitted across the network.

node_1 is the IP book icon used to assign IPv4 addressing to subnets.

node_2 is the workstation from where both transmission and processing takes place.

node_3 is the server which executes the instructions processed by node_2.

node_5 is the Virtual Private Network from where the data can be flown to other networks.

node_6 is the Hub using which more number of clients can avail Internet services.

Server data(node_3) is available at all the other nodes particularly by node_0, node_1, node_2, node_5 and node_6. Node_0 is the Lan accessible to many nodes. node_2 is the work station from where data is processed to other nodes and the server. node_5 is the Virtual Private Network used to transmit data over several networks. node_6 is the hub that is used to access Internet. The possibilities of accessing data from node_1(Fig.5.1.), accessing data from node_2(Fig.5.2.) and from node_3(Fig.5.3.) are given below.

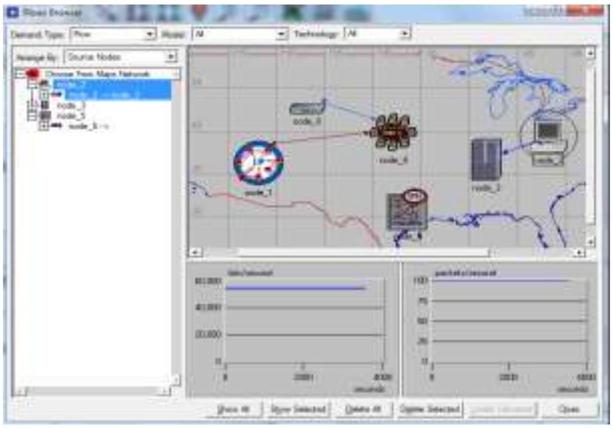

Fig.5.2. Traffic Flow from node_2

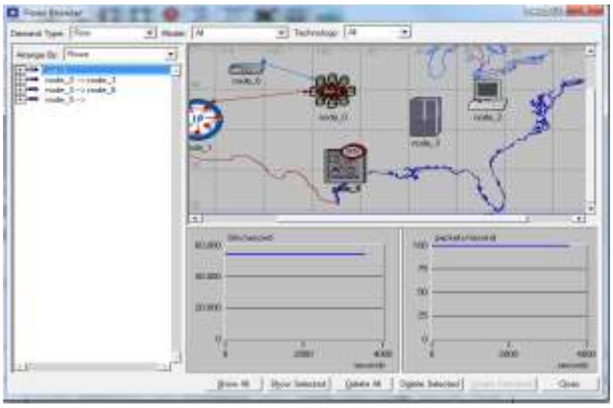

Fig.5.3. Traffic Flow from node_1

The prototype for data capturing process is developed using OPNET modeler. This modeler is convenient for tracking packet flow and for modeling data flow from centralized server to its workstations.

Table 5.1. Benefits of Proposed methodologies

Sl.No.	**Methodology name**	**Fringe benefit**
1	Traffic analysis at routers	Traffic analysis is done using sensors to facilitate automatic alerts.
2	Identifying the types of attacks	Adoption of micro sensors and motions sensors at ISO layers provides security layerwise.
3	Handling Localization issues	Keeps track of geographic locations through mobile sensors.
4	Incorporating Cluster Head mechanism.	Cluster based message transmission helps in quick message transmission.
5	Managing Routing Protocols	The decoding of header information is accurate if the message transmission is by using RFID tags or sensor.
6	Checking for integrity of the data received	Intra cluster communication through Bluetooth communication helps in avoiding integrity violation as the intra cluster distance is very small which results in accurate transmission.

VI. CONCLUSIONS

By applying possible solutions at various levels, the intensity of data sensing by the attackers can be minimized. And by applying Aggregation techniques using sensors, the threat of against attacks in accessing confidential data is stopped.As Sensors are used to collect information about the data sensed, transmission range of sensors is the focal point. The restriction to this paper is as sensors are battery powered; they have short range sensing capability. This concept can be extended by applying ultraviolet sensors and by refining the solution of possible vulnerabilities in attacks to protect security.

VII. REFERENCES

[1] L.ToddHeberlein,GihanV.Dias,KarlN.Levitt,Biswant hMukherjee,Jeff Wood and David Wolber,"A Network Security Monitor",Division of Computer science,Dept.of Electrical Engineering and Computer Science,University of California,Davis CA, Research in Security and Privacy, Proceedings., IEEE Computer Society Symposium on 7-9 May 1990.

[2] Andreas Larsson,"Security and Self-stablilization in Sensor Network Services,Division of Networks and Systems",Department of Computer Science and Engineering,Chalmers University of Technology,Sweden 2012.

[3] Kumar Nikhil and SwathiAgarwal and PankajSharma,"Application of Genetic Algorithm in Designing a Security Model for Mobile Adhocnetwork",Department of IT,ABES Engineering College,Ghaziabad(U.P),India.

[4] Jamal N. AI-Karaki Ahmed E.Kamal,"Routing Techniques in Wireless Sensor Networks:ASurvey",Department of Electrical and Computer Engineering,lowa State University,Ames,lowa 50011

[5] Prof Ram Meghe et al,"Database Tampering and Detection of Data Fraud by Using the Forensic Scrutiny Technique", ISSN 2250-2459, ISO 9001:2008, Volume 3, Issue 2, February 2013.

[6] ToshishigeShimamura et al,A Fingerprint Sensor with Impedance Sensing for Fraud Detection,2008 IEEE International Solid-State Circuits Conference - Digest of Technical Papers,University of Pennsylvania,3-7 Feb. 2008.

[7] V.Priyadharshini et al,Prevention of DDOS Attacks using New Cracking Algorithm, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2263-2267.

[8] Ms. Madhavi N. Shrikhande et al,EMBEDDED WEB TECHNOLOGY IN TRAFFIC MONITORING SYSTEM, International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 4 (May 2014).

[9] V.Ilango et al, Cluster Analysis Research Design model, problems, issues, challenges, trends and tools,

International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397 Vol. 3 No. 8 August 2011,pp 3064-3070.

[10] NisheethShrivastava et al, Medians and Beyond: New Aggregation Techniques for Sensor Networks, SenSys'04, November 3–5, 2004, Baltimore, Maryland, USA. Copyright 2004 ACM 1-58113-8 79-2/04/0011 ...$5.00.

[11] SumitChaudhary, Energy Efficient Techniques for Data aggregation and collection in WSN, International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.4, August 2012.

[12] Cynthia Dwork et al,Rank Aggregation Methods for the Web,Copyright is held by the author/owner. WWW10, May 1-5, 2001, Hong Kong. ACM 1-58113-348-0/01/0005.

[13] CHEE-YEE CHONG et al, Sensor Networks: Evolution, Opportunities, and Challenges, PROCEEDINGS OF THE IEEE, VOL. 91, NO. 8, AUGUST 2003.

[14] Saroj et al, Study on Various Clustering Techniques, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 3031-3033.

[15] AbhaDamaniet al, Global Positioning System for Object Tracking, International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 8, January 2015.