

Customized Mechanism to Detect, Monitor and Block Data Packets Selectively

¹Anjamma Nomula ²Dr.R.V.Krishnaiah

¹ Dept of CSE, JNTU H, DRK Institute of Science and Technology, Hyderabad, Andhra Pradesh, India
Principal

² Dept of CSE, JNTU H, DRK Institute of Science and Technology, Hyderabad, Andhra Pradesh, India

Abstract: Computer networks need security in place to protect IT systems. As computer networks are everywhere, it is essential to have a mechanism for selective data stream blocking. This paper presents a tailor made mechanism that is responsible to monitor, detect and block as per the definitions associated with the customized mechanism. The proposed mechanism blocks data packets after verifying the protocols that govern the proposed mechanism. The empirical results revealed that the mechanism is robust and can be used in the real world networks.

Keywords: data packets, packet sniffers, intrusion detection, firewall, data stream

I. Introduction

First of all computers were standalone and have no business with other computers. Now the situation is totally changed and computer can't stand alone and needs to be connected to other system to form a network in order to reap benefits such as sharing of resources and information. The term network does mean that [1] a set of interlinked lines to form a net. For instance network of roads, network of telephones, and network of airlines and so on. However, the computer network is a network which has two or more computers interlined for sharing information and resources. Such networks are of many types again. Each network should have a protocol or a set of rules and regulations to be followed by both server and client machines that reside over network. The networks are classified into LAN, MAN, and WAN. Apart from this networks may be wired or wireless and with further classifications in turn. Whatever be the form of computer network, the data is flown over network. It does mean that data streams are being transmitted. The origin of data stream might be a computer in the local area network or any other system that is somehow associated with network. The data flow over network has to be monitored for security reasons. In case if any adversaries and certain attacks are suspected, the data streams are to be blocked. The communication path at network layer can be interrupted and let the data packets to identify themselves. As an alternative, the nodes can try to find information themselves. It can be achieved by analyzing the application layer and which is part of data communications [2]. The drawbacks of the both methods include:

- It is not possible to gather user information in either active or passive fashion.
- Performance gets reduced if passive gathering of information is involved and it also involved implementation effort.

II. The Need For Customized Mechanism

Both active and passive approaches are two extremes. There exists an approach between these two extremes in which the applications and data packets are monitored and thus overcoming drawbacks and disadvantages that are prevailing with respect to existing techniques or methods [3]. Thus the proposed mechanism acts like a bridge between the active and passive mechanisms that paves the way to a robust way of blocking data packets that are being flown over network.

III. Techniques Used As Of Now

As of now the technologies used in the area of networks include closing down network switches closely; banning data transfer, making use of a network sniffer; the usage of firewalls; and intrusion detection systems. These are essential technologies required by the prototype application. To prevent data stream circulation over network, it is essential to prohibit particular kinds of applications or the corresponding data streams from getting circulated over network. To block data streaming another technique is to leave the network with limited connectivity or no connectivity. Network sniffer can also be used that can intercept and log the packets moving around over network. As data is flown over network the sniffers [4] examine the packets and block if necessary. Firewall is another security approach that automatically monitors the incoming and outgoing packets that are being flown over networked nodes [5]. This security mechanism is capable of blocking data streaming selectively. Firewalls are of many types. They include packet filtering, circuit relay, and application

level gateway. In this kind of firewall only address information and protocol of each packet are verified. The context of the packets and their content are ignored. In the local network and host firewall does not pay any attention towards sources of incoming data.

As per [6] the filtering is a process of verifying incoming and outgoing data packets over network and taking decisions based on rules and policies weather to allow them or deny them. Circuit relay is another kind of firewall where connections are validated before allowing data exchange. Instead of allowing or not allowing packets simply, it also verifies the validity of connections among the nodes and takes decision if the source and destinations are legal. Based on the factors like destination IP address, protocol, user, port, and password, source IP address whether a connection is valid or not is determined [7]. Application level gateway [6] works at the application level of the backbone of network i.e. TCP/IP. As expected it verifies all incoming and outgoing packets at application level only. The gateway automatically drops the packets which are not valid. They also ensure that unwanted traffic from outside sources does not enter into the network [7]. It never routes any traffic on the network layer of OSI model. All the data stream packets are stopped at gateway and then routing decisions are made if they are valid. Otherwise the packets are discarded.

Intrusion detection systems are tools that ensure secure communication in networked nodes. They monitor network flows and find any malicious data is flown among the networked systems. This tools works like a sniffer that can detect malicious content being flown. It is capable of verifying signatures and VIRUS and then logs the details for future retrieval and revisions. Table 1 summarizes the disadvantages of all the techniques discussed so far.

Table 1 –Various Techniques to Block Select Data Packets

TECHNIQUE	DISADVANTAGE
Network Sniffers	<ul style="list-style-type: none"> • Its drawback is that it can leave data susceptible to exposure. • Hackers can use this technique for obtaining sensitive information. • Access rules are complex and it is not flexible to operate. • Communication state is not maintained. Packets are considered but not the context of the actual traffic.
Packets Filtering	<ul style="list-style-type: none"> • Lets users connect to network directly. • Data allows security problems to happen. • The security policies are not user friendly.
Circuit Relay	<ul style="list-style-type: none"> • Operates at transport layer and programming modifications are required. • It only focuses on parties involved in communication instead of examining packets. • Behind the firewall clients should be proximatized so as to obtain services.
Application Level Gateway	<ul style="list-style-type: none"> • Needs multiple services and thus slow in response. • Multiple programs are required in order to block a class of applications. • Clients are to be proximatized to make use of services.
Intrusion Detection System	<ul style="list-style-type: none"> • As each and every packet is verified, it functions slowly. • Not suitable for real time data packet transmission.

IV. Proposed Mechanism

The aim of the proposed mechanism is to monitor and detect data packets that need to be blocked selectively. The strategy followed to achieve the aim is to identify target applications and develop a rule/definition bank that is used for blocking data stream selectively. The checking data packets' process is done in two different phases. Header inspection is the first phase while the second phase is that the packets are to be matched with the sample packets. Only the packets whose header packets are suspected. Freeway is another concept in which if packets initially shows the proof of evidence that they are genuine, the subsequent packets are allowed without verification. Aging is another technique which is modeled after process synchronization. All data transmissions are kept in queue. Before sending data from one node to another node it gets verified

now. After reaching some threshold data packets move into freeway. However, priority decreases because the time is increased. The priority is known as immunity. The process comes back in queue in order to get immunity. Thus the aging principle is implemented in an improved form and perspective. The features of proposed solution and their advantages are as given below.

Freeway—Once a stream is verified sometime, the packet flow is not interrupted for the purpose of checking.

Aging—infinite transmission from a connection is prevented.

Header Check—used to achieve increased throughput and speed.

The criteria and corresponding advantages are as given below.

Accuracy—The proposed mechanism achieves more accuracy in finding the data streams that are to be blocked selectively.

Security—The proposed architecture causes the operations like spoofing and masking to fail

Maintenance—Maintenance is easy as the mechanism expects only sample data packets for updating database containing definitions.

Speed—The dynamic mechanism yields lower speed while the customized mechanism yields higher speed. We preferred the latter keeping the aim of the paper in mind.

V. Experiments

The experiments are made by using a customer simulator application. The environment and the functionalities of the application are as described below.

i. Environment

The environment used to build customer simulator that demonstrates selective data stream blocking mechanism for networks include a PC with 2 GB RAM, 2.93 GHz processor, JDK 1.6 (JSE 6.0) for simulator development, Eclipse as an IDE (Integrated Development Environment). Java programming language, especially its SWING package and networking packages are used to build the functionality of the prototype application.

ii. Custom Network Simulator

The application developed to simulate an environment where selective data stream blocking mechanism for networks is demonstrated has the user interface shown in fig. 1 for vehicular network represents a CAR.

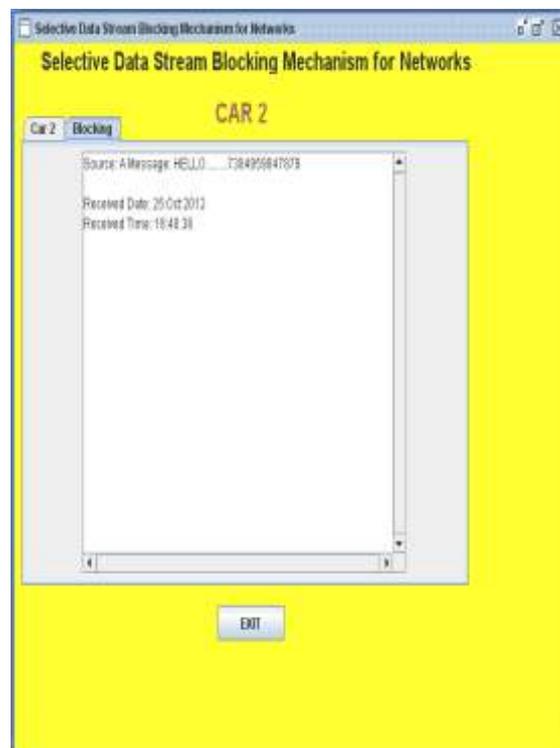


Fig. 1 – CAR screen of vehicular network

As can be seen in fig. 1, the UI which represents CAR in the vehicular network is capable of sending messages to any other car in the network. However, the messages go through a road side unit which acts as a

router. The aim of this paper is to have mechanisms for selective data stream blocking for networks. Towards this end, the blocking option is used. The UI of road side unit in the vehicular network is represented as figure shown below.

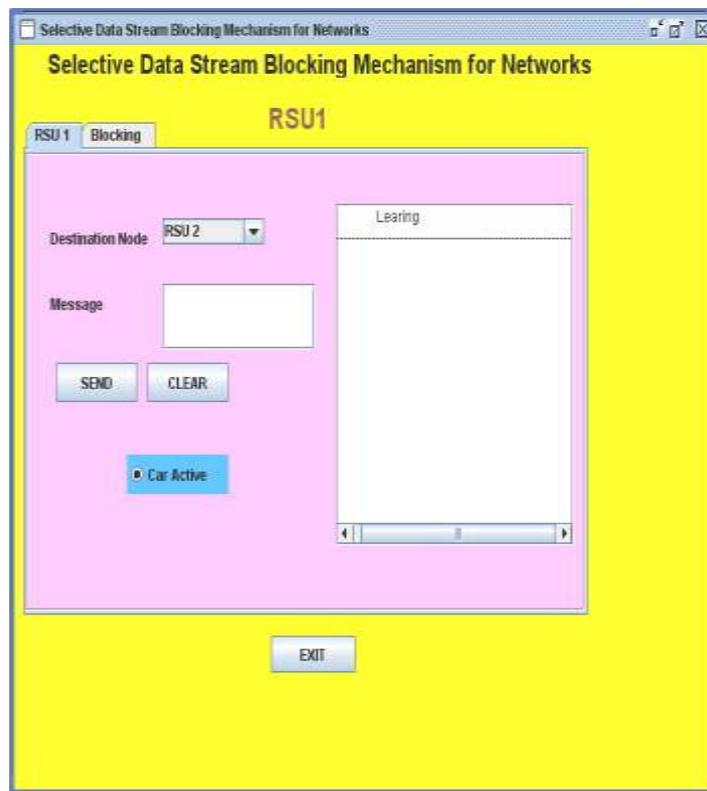


Fig. 2 – UI of road side unit in vehicular network

As can be seen in fig. 2, the screen represents road side unit of vehicular network. It has provisions to send messages to other road side units and also cars in the network. It can send messages to active vehicles and also act as router between the vehicles. It does mean that when a vehicle sends message to other vehicle that message goes through the router that is road side unit. RSU can also block the messages when it is busy. The blocked messages are viewed here. The blocked messages are resent when it is free again. Selective data streaming is what happens as described in this paper. When messages are arrived to router, it presents them on the screen as shown in fig. 3.



Fig. 3 – RSU showing messages

When messages are blocked as per the mechanisms discussed in this paper, they are presented in a graphical window. The blocked messages and other relevant details are presented in a text area. The listening option in the main window lets router listen for incoming data and report number of packets reached at the router and number of packets yet to be sent to the intended destination. The learning option in the main menu lets the router to report you that from whom the data or packet has come and whom it has to be reached and

what data to be sent to the destination. The switching option in the main menu lets the switching operation in the router module is used to forward the packets to the destination. The operations it handles include forwarding, discarding and filtering. Forwarding lets packet or data which kept stagnant at the router for long time to be forwarded to destination. Discarding lets Packets which need not be sent to the destination to be deleted at the router itself. Filtering lets packets or datagram's at router to be sent to any other destination.

iii. Observations

Packets from the router machine are received at destination machine and these they are reassembled into original message and written into a file with destination machine name. However, the demonstration of selective data stream blocking mechanism for networks.

VI. Conclusion

With respect to network and security aspects, this paper presents a new customized mechanism meant for detecting and blocking data streaming selectively. This is because the dynamic model lowers speed while customized mechanism gives higher speed. In the proposed approach user can determine which kind of mechanism to be deployed keeping the cost in terms of speed in mind. The experimental results revealed that the proposed customized mechanism yields good results in terms of speed and blocking as discussed in this paper.

References

- [1] *The New Lexicon Webster's Encyclopedic Dictionary of the English Language*. New York: Lexicon.
- [2] Associating Network Flows with User and Application Information, Ralf Ackerman, UtzRoedig, Michael Zink, Carsten Griwodz , Ralf Steinmetz, ACM Multimedia Workshop, 2000, Marina Del Rey CA USA
- [3] Detecting Intruders on a Campus Network: Might the Threat Be Coming From Within? Rich Henders, Bill Opdyke, SIGUCCS'05, November 6–9, 2005, Monterey, California, USA
- [4] A Taxonomy of free network sniffers for teaching and Research, Victor A Clincy and Nael Abu-Halaweh, JCS 21, 1(October 2005), Midwestern Conference, Consortium for Computing Sciences in Colleges
- [5] A History and Survey of Network Firewalls, Kenneth Ingham, Stephanie Forrest, The University of New Mexico Computer Science Department Technical Report 2002-3
- [6] Evolution of the Firewall Industry, Cisco Documentation, Network Security
- [7] While Paper, Firewall Software and Internet Security, 2002 Vicomsoft Ltd

AUTHORS

	Anjamma Nomula is student of DRK Institute of Science and Technology, Hyderabad, AP, INDIA. She has received B.Tech Degree computer science and engineering, M.Tech Degree in computer science and engineering. Her main research interest includes data mining, Software Engineering.
	Dr.R.V.Krishnaiah (Ph.D) is working as Principal at DRK INSTITUTE OF SCINCE & TECHNOLOGY, Hyderabad, AP, INDIA. He has received M.Tech Degree EIE and CSE. His main research interest includes Data Mining, Software Engineering.