ISSN No. 0976-5697

Volume 6, No. 6, July - August 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Hop-By-Hop Encryption Protocol for Transmission of Data over Public Networks

Subhash S[1], Dr. Santosh Deshpande[2]
PG Scholar[1], Professor[2], department of PG studies, VTU, Belagavi, Karnataka, India
subhashgowda01@gmail.com, sld@vtu.ac.in

Abstract: Internet is becoming most popular since past decades for its wide beneficial features. It is used as main source as media of communication and consists of many public networks. Therefore, the user data needs to go through public networks. As a result, to maintain the effectiveness and the consistency of applications, faster data delivery and data integrity are crucial. The Service-oriented-Router (SoR) was introduced to maintain the rich information on the Internet also, to achieve maximum benefit from networks. Specifically, the security, privacy and integrity of communication are not discoursed despite of its significance brought by its underlying personal vital information. A SoR can analyze all packets or network stream transactions on its interfaces and hop-by-hop routing protocol which gives hop-by-hop data encryption using functions of the SoR. This infrastructure can provide security, privacy and integrity by using these functions.

Keywords— hop-by-hop encryption, hop-by-hop FEC, hop-by-hop routing, hop-by-hop tunneling, Service-oriented Router.

I. INTRODUCTION

The public networks are less secure because they are accessible by any one, hence it is generally termed as public network. Due to it is contrasted to private network; it is more vulnerable to security attacks because of its limited constraints or no constraints on access. Hence while transmission of any data over public networks; there must be a need of security to that data. In today world, most of the networks are using the internet to achieve some desired task. The internet comprises of many public networks, so there is a need of much security in addition to already existing security mechanisms. So the proposed system called hop by hop encryption using service oriented router does solve above issues.

The assuring of data integrity is also an important factor for the data transmission over public networks mean while diminishing the processing delay. The proposed service oriented router [1][2][3][6][7] is new generation router, which is capable of analyzing the packet data contents. An SoR consists of high throughput database and is capable of analyzing all transactions on its interfaces. Moreover, SoRs can posses APIs in order to access the stored contents to enhance services. One of the main goals of this protocol to give function to transfer data more securely and with assured integrity over the public networks. Since final result is based on the consistency of data transmission and delay in data transmission.

SoR is designed with intension to work as any class of network router, its configuration of software and hardware meet 2Gbps data traffic found on the Alaxala and juniper routers. Therefore, the additional processing power needed for decryption and encryption processes for protocol which is used in the SoR wouldn't affect to delays caused while data transmission. Since security, low transmission delays and integrity are the most important parameters to be considered in any system which deals with transmission of data over public network.

As the internet turns out to be popular and wide spread, it is turning into a large data source of millions of users, where data are disseminated by internet router. A router is a fundamental device that connects various autonomous networks and directs data from source to destination node. A normal router does not provide content based services and this restricts advantages of service providers and data carriers. Data is useful and valuable because providers of content based services can develop numerous enhanced services with it. Co-existence among providers of internet contents and internet carriers will be vital theme of internet. Since the router is responsible for interconnecting various networks, a router can get any sort of data incorporated in packet streams: L2 and L3 information, information of packet header, application information, and so on.

Furthermore, data or content can be gathered passively by a router. An SoR can give services, accessible through an APIs to users. An SoR has numerous merits, as an instance of it is that data can be gathered passively. Unlike present end-to-end systems that must gather data actively. In dynamic data gathering, end hosts can obtain required data just by getting to different hosts, for example, search engine web crawler. This requires some time and scope of data correction is constrained. Frequent crawling to acquire the real time circumstance of the internet can lead to network congestion. The data collected passively by the SoR empowers ongoing data acquisition and provides present status of the internet.

Using previously stated services, application and service developers give quicker and more viable communication to their clients. Moreover, passive data collection and keep up gathered data in speed data bases will give rise new era of giving services from the edge routers. As a case, in request routing of DNS-based content delivery network, clients need to wait till information about the redirector sent by the name servers and the redirector discovers surrogate servers information. This expands the time of initiation connection. Essentially every time user changes requests for a new content or surrogate server being updated, truly time of response will be increased because of DNS determination.

If SoRs substituted with edge routers and present communication protocol of surrogate server, SoRs can recognize the location of surrogate servers and clients can significantly connect to their edge SoR rather than resolving DNS. This makes initiation of connection speedier. In addition, SoR can be programmed to give benefits as

content filtering, websites recommendations for contents and picturize content flows and internet access patterns can be monitored from SoR itself. In this way, the SoR has capability of making open innovation platform by giving APIs in order to develop applications by serving clients successfully and quickly. In the area of networking, there are numerous areas of research like virtual experiments on new network concepts, analysis of new designs, development of new protocols and other preliminary evaluations. In this study, we present a routing protocol which is based up on the SoR functions. The implemented protocol for secure data transmission comprises of the following: Recognizing the neighbors, per hop key exchange, maintaining distributed key table in each SoR and decrypt and encrypt packets on departure and arrival from/to SoR.

II. METHODOLOGY

A. Hop-by-Hop encryption in Service-oriented Router (SoR):

When coming to encryption, there are two kinds namely end-to-end encryption and link encryption. In end-to-end encryption, only encryption of payload will be takes place but not the headers and trailers are encrypted. These headers and trailers remain readable. This creates vulnerabilities in getting accessed to information, such as source or from the point where the packet is moving towards and what kind of data which is carrying. Since the headers are not encrypted in end-to-end encryption, the attacker or anyone can get to know the information about source and type of data in packets. But in the case of link encryption, not only the data is encrypted, along with headers and trailers are encrypted irrespective of the protocol or the content.

In communication, most of the cases we use end-to-end encryption in SSL and SSH. Moreover, we often use link encryption in technologies such as point-to-point tunneling protocol and MACsec especially in satellite communications and in T3 lines. In end-to-end encryption, initially the connection at end-to-end will be established between two parties. Next these two parties will share key among them using relevant method. After which data will be sent via chosen path which is optimal after the encryption of data using shared keys. Secure communication will be established because the decrypting keys are only known to the communicating parties.

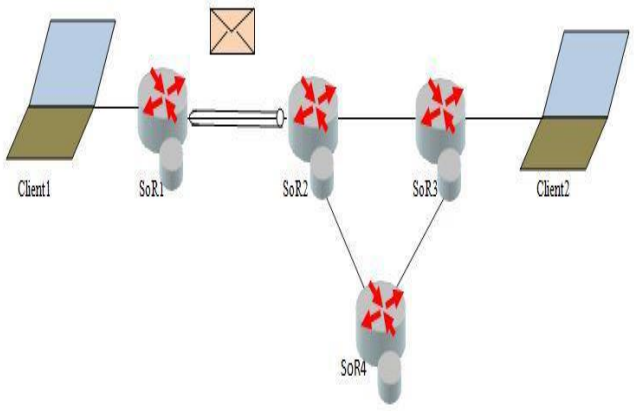

Figure 1. Hop-by-hop tunnel in SoR based network.

Contrast to end-to-end encryption, the proposed system called hop by hop encryption does the encryption of data during its transmission via the network. It is shown in fig 1. The tunnels are created when the packets transmission occurs between the SoRs dynamically in the network. When packet arrived at SoR1 from the client1, tunnel will be created between SoR1 and SoR2. After the packet reached at SoR2, appropriate path will be selected based on its routing table and at the same time tunnel will be created in that selected path and finally packet will reach the destination client2.

B. Advantages of proposed System:

a. The proposed hop-by-hop routing protocol will be able to provide both secured routing and ordinary routing simultaneously for both the general packets and motion control data packets transmitting through the public networks.
b. The most efficient and effective path can be selected according to the real time link conditions.
c. This will speed up the packet transmission while optimizing the congestions in the wide area networks.

The protocol will allow transmitting both ordinary packets of the network and also the packets that need to be securely delivered via encryption simultaneously.

III. PROPOSED HOP-BY-HOP ENCRYPTION PROTOCOL DEVELOPMENT

In the proposed system, as soon interfaces in the SoR up, mean time hello packets are exchanged among the neighbors to indicate new interfaces. Though, this exchange of hello packets, neighbor table will be created by SoRs. After which SoRs will distribute key at each and every interface. To do this RC5 algorithm used to exchange the key securely and to create neighbor table. After exchange of key, SoR will manage the key in its own key table. At the same time SoRs will also transmit the routing updates to create their routing tables. The encryption of the packet is as illustrated in fig 2. The proposed system chooses the best path based on its real time conditions and least cost. Whenever the packet needs encryption including header, the protocol need to choose its own header structure and always it copy the sender and receiver details in its header. Then sender and receiver portion in the header will be replaced by present forwarding interface with obtained interface of next hop SoR. This will provide the potential to route the packet to the shortest path. Henceforth data as well as details of sender and receiver remains unreadable by any other device other than destined next hop which has the key to decrypt data and header in the packet.

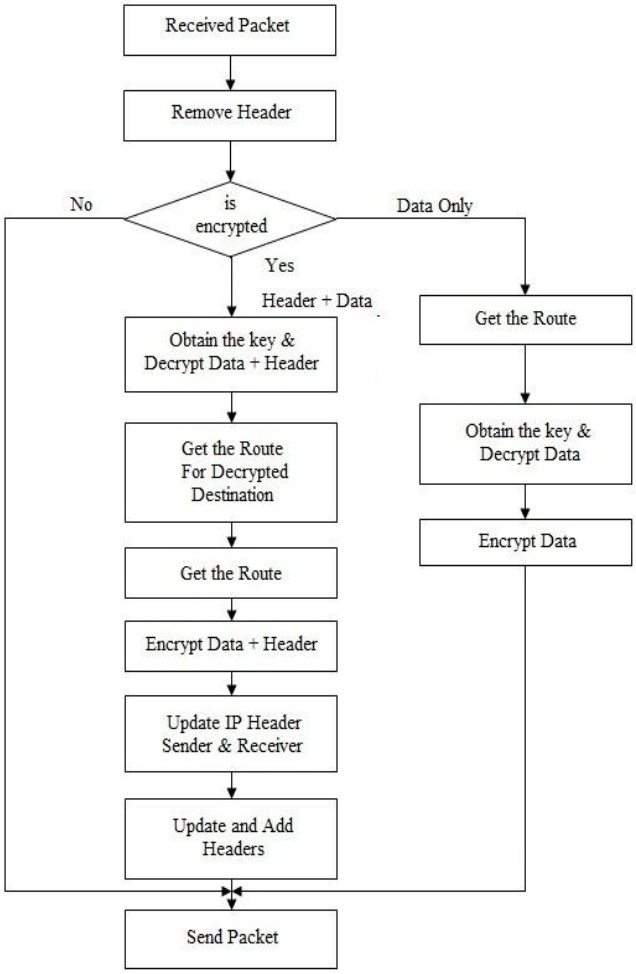

Figure 2. Flow chart for packet encryption process.

In the case of any communication which require only data to be encrypted without other information, only data will be encrypted by the proposed protocol and send it to the next hop along with its IP header and other SoR header information to identify the next hop SoR. The header of SoR will contain unique fields to identify each packet type. Upon successful reception, decryption takes place only if the packet is encrypted by the previous hop using the same key obtained from its key table. After reading the details of sender and receiver, if in case the received packet in current SoR is not particular receiver of the packet then have to do above process after choosing the appropriate next hop to forward data. If the packet need encryption then it will be encrypted by following above process and it will send the packet to appropriate next hop SoR. This procedure will continue till the packet is reached to destination. Finally details of sender and receiver are updated in IP header and receiver gets the same packet as at the source. The main merit of this method is that most effective and efficient path will be chosen as per the real time link conditions results in speeding up the packet transmission and minimizing the congestion in WANs. The protocol can be used not only for the data which needs to travel more securely over public networks, which also allow the ordinary packets to travel over the public networks.

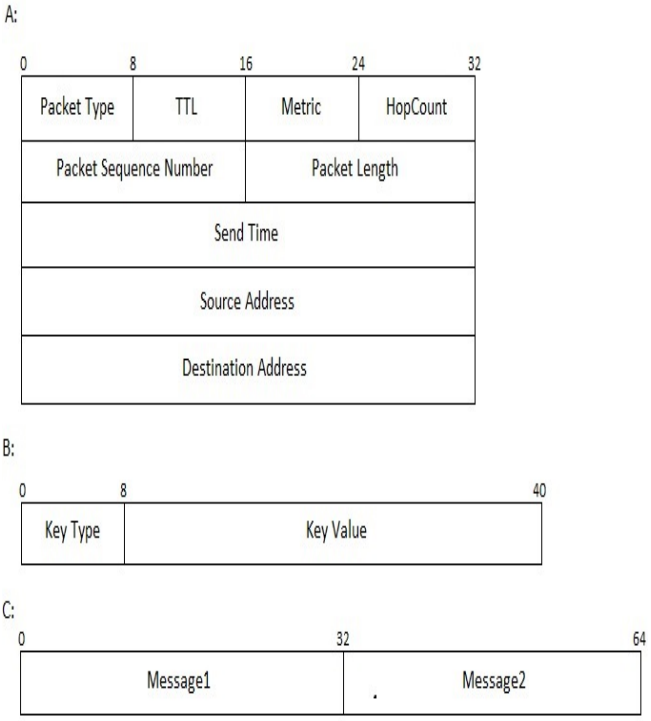

Figure 3. Packet header structures used in the proposed protocol.

During transmission of packets through the network due to congestion or unpredictable network behavior, packet may get lost, receive in out of order or duplicated. When considering any network, data to be transmitted more securely by preserving integrity of data with minimal delay as much as possible. Obviously there are many possibilities for the error to be occurred while transmission of packets through the network. Nowadays those circumstances can be borne using functionalities such as forward error correction [4][5].

In those methods, the error can be corrected by requesting the original data from the source. Therefore the retransmission delay is the most significant factor for any application to respond to the users as quick as possible. Even though error can be corrected using conventional FEC, it affect time sensitive applications. However in the proposed protocol, it can be installed in every SoR. So that, each SoR will contain the copy of packets or reference of it in span of certain time window. Therefore if any error is occurred while transmission and is detected by SoR then the request can be sent to previous SoR by using hop by hop FEC instead of requesting the originator where the packet transmission began. Hence this method can significantly reduce the retransmission delays.

Figure 5 shows input configurations and output results. Observation made from the below results is some amount of energy consumption reduced which is also depends on number of cycles per second of the network. The packet delivery ratio is also found optimal.

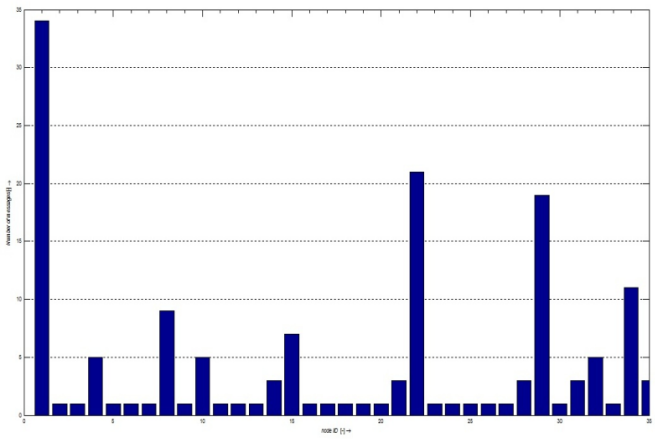

Figure 4. Packet transmission ratio graph

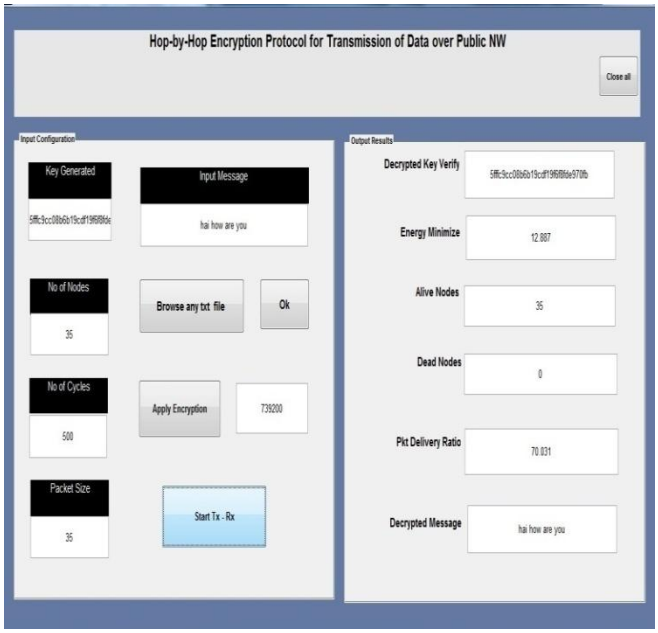

Figure 5. Input Configuration and Output Results

IV. CONCLUSION

We presented hop-by-hop encryption protocol which can be utilized in application which does transmission of data over public networks. The proposed system is developed with intension to make network to route the packet to the destination through shortest path and also encrypting the data to route more securely, both of these achieved. Along with shortest path discovery and encryption of data, some amount of energy is also minimized and packet delivery ratio got optimal. In future, hop-by-hop FEC can be developed so that loss of data because of bit errors can be minimized significantly. Likewise, we can develop a Certification Authority (CA) based authentication system which can minimize the threats, which are occurred when fraud SoRs are added to the Network.

V. REFERENCES

[1]. Y. Nagatomi, M. Koibuchi, H. Kawashima, K. Inoue, H. Nishi, "A Regular Expression Processor Embedded in Service-Friendly Router for Future Internet," in Proc. 39th International Conference on Parallel Processing Workshops (ICPPW), pp.82—88, Sept. 2010.

[2]. K. Takagiwa, S. Ishida, H. Nishi, "SoR-Based Programmable Network for Future Software-Defined Network," in Proc. IEEE 37th Annual Computer Software and Applications Conference (COMPSAC), pp.165—166, July 2013.

[3]. K. Ikeuchi, J.Wijekoon, S. Ishida, H. Nishi, "GPU-based Multi-stream Analyzer on Application Layer for Service-Oriented Router," in Proc. IEEE 7th International Symposium on Embedded Multicore Socs (MCSoC), pp.171—176, Sept. 2013.

[4]. H. Sato, T. Yakoh, "A real-time communication mechanism for RTLinux," in Proc. 26th Annual Confjerence of the IEEE Industrial Electronics Society (IECON2000), vol.4, pp.2437—2442, 2000.

[5]. P. Kihong, W. Wang, "AFEC: an adaptive forward error correction protocol for end-to-end transport of real-time traffic," in Proc. 7th International Conference on Computer Communications and Networks, pp.196—205, Oct 1998.

[6]. Inoue, K.; Akashi, D.; Koibuchi, M.; Kawashima, H.; Nishi, H.; "Semantic router using data stream to enrich services," Future Internet Technologies (CFI08) Seoul, Korea, June 18-20, 2008, Proc. International Conference on, pp. 20–23.

[7]. Wijekoon, J.; Harahap, E.; Nishi, H., "SoR based request routing for future CDN," Application of Information and Communication Technologies (AICT), 2012 6th International Conference on, pp. 1, 5, 17-19 Oct. 2012

[8]. Junos V App Engine - Network Virtualization Software Platform - Juniper Networks, http://www.juniper.net/us/en/productsservices/software/junos v-app-engine/

[9]. D. Mitzel, Overview of 2000 IAB Wireless Internetworking Workshop, RFC 3002.

[10]. H.Balakrishnan, R. H. Katz. "Explicit Loss Notification and Wireless Web Performance" Proc. IEEE GLOBECOM'98 Internet Mini- Conference, Sydney, Australia, November 1998