International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 4, Volume 2 (April 2015) www.ijirae.com

Implementation of Hop-By-Hop Encryption Protocol for Transmission of Motion Control Data over Public Network Using Sors

RAVIKUMARA V*
CSE & VTU

LAKSHMIKANTH D B
CSE & VTU

Abstract— Bilateral teleportation System is combination of both robot technologies and the sensor network this is widely used in to perform the operation remotely. The bilateral control system to perform the surgeries in remote location without visiting the actual place. The application using bilateral can be found in the area of outer space exploration, toxic material and minimum cost surgery because of existence of time varying delay in the communication, due to long distances and unexpected disturbance causes some problem. The existence communication time delay may destabilize the master- slave teleoperation system. In our propose system the control a specific surgery robot the robot will send the data remotely and communicate sending control data through the network. The system will do surgery like same location where surgeon is performing the operation. A hop-by-hop routing protocol is implemented and data is encrypted to provide data security and integrity in the public networks using SoR. The processing delay is reduced by 46.32 µs per packet with the help of protocol for encryption and decryption of the packet.

Keywords- Service Oriented Router, Hop-by-Hop Routing, Motion Control Over Networks, Bilateral Controllers, Processing Delay

I. INTRODUCTION

In computer networking, a *hop* is one portion of the path between source and destination. Data packets pass through bridges, routers and gateways on the way. Each time packets are passed to the next device, a hop occurs. Complexity of the communication of the network, the delay of the data packets not only the time varying but also it is very important to investigate the asymmetry. The hop count refers to the number of intermediate devices through which data must pass between source and destination, rather than flowing directly over a single wire. Each router along the data path constitutes a hop, as the data is moved from one Layer 3 network to another. Hop count is therefore a basic measurement of distance in a network.. The transfer of data among teleoperation system is highly sensitive and critical so the delays in transfer of packets have to be reduced and be accurate in the transfer of data.

Critical and Sensitive data is transferred in teleportation systems. A minor modification to the data can end up in the failure in the operation this may lead to the end of the life of a human being. Ensuring the secure data delivery plays a very vital role in these types of applications. The overall delay has to be minimized in the bilateral transmission of control data over the network. The integrity of data is important in these types of applications. Bilateral control systems enable the surgeons to perform the surgeries in a remote location without visiting the actual place where the surgery has to be performed.

The major drawbacks [1] in the existing approach:

1. *The packet loss is very high in the network.*
2. *The variable delay in the transfer of data packet in the bilateral communication(High jitter)*
3. *Transmission delay in the transfer of packets from source to destination*
4. *High transmission bit error*
5. *Network reliability is not maintained in the existing system.*
6. *Data Security, Integrity and Privacy are less in the existing system.*

The advantages of using proposed system is:

1. *Processing delay is less than 45.32* ***µs .***
2. *The data encryption provides data security from attackers*
3. *Network Reliability is achieved if there is a failure in the node it takes alternate path to reach the destination*
4. *Low packet loss, low jitter, low total delay and low bit error*
5. *Service Oriented Router is a new generation backbone router which can inspect the data contents in a packet up to OSI layer.*

II. RELATED WORKS

Next generation surgical robots under development at the University of Washington [2] BioRobotics Laboratory and at SRI International will allow surgeons to perform robotic based Minimally Invasive Surgery remotely. Teleoperated surgical robots, or telesurgical robots, will allow highly trained medical personnel to provide skilled care from distant locations.

This capability may be used in civilian settings to allow surgeons to care for patients in underserved remote locations or in disaster areas. Ultimately, telesurgical robots will be deployed into the battlefield to provide nearly immediate medical assistance to wounded soldiers. The Secure ITP addresses security issues for ITP based telesurgical robots allowing security to be deeply implemented in these complex cyberphysical systems. It addresses four security elements: communication, authentication, authorization, and security policy development and enforcement.
Shares the symmetric key with others any one can retrieve the data.

Service-oriented router [3] is new router architecture for providing rich services to Internet users by utilizing useful information extracted from network traffic. In SoR, stream reconstruction and selection is a fundamental process for providing the services in the application layer. After real-time reconstruction of stream data, SoR used a software character string analyzer to extract important required information. One of the promised services is a router-level network intrusion detection system. Because a network consists of hundreds of thousands of data streams, achieving an intended throughput while analyzing these stream data is a critical problem. We propose an acceleration method of string matching based on a heterogeneous system consisting of a CPU and a graphics processing unit. In addition, we designed and implemented a task controller that improves the distribution of POSIX-thread-based processes so that string matching can be performed concurrently depending on the status of the string matching system.

TCP is a [5] reliable transport protocol that has been tuned to perform well in networks where packet losses occur mostly because of congestion. However, wireless networks are different: TCP responds both to congestion-based and errorbased losses by invoking congestion control algorithm and reducing the sending rate, resulting in degraded end-to-end performance for wireless systems. We investigate a new end-toend approach for improving TCP performance over lossy links by using adaptive, end-to-end forward error correction for recovering losses and consequently avoiding the TCP back-off behaviour. Of course there is a clear trade-off between the capacity consumed by FEC and the gain achieved in the overall throughput. An adaptive algorithm is needed to calculate the optimum ratio of redundancy given the state of the connection. The sender uses feedback information from the receiver to dynamically tune the FEC parameters. Through simulations we evaluate the performance of TCP with end-to-end FEC in mixed wired and wireless networks. The simulation results show in different scenarios that the throughput can be significantly improved by adding end-to-end FEC to TCP. However, compared to other improved TCP variants such as Westwood the performance is not improved, hence a direct modification of TCP congestion control appears to be more efficient than adding end-to-end FEC.

Linux has been effectively used as a reliable operating [4] system in workstations and servers. However, the interest for using it in embedded systems has grown recently, due to the easiness for customizing it and the availability of the source code. This paper describes the experience of customizing RT-Linux for its use in an embedded real-time control. The main issues involved in this task are outlined and the adopted solution is described. These issues include the system configuration, the minimization effort and how to achieve real-time features through the use of RT-Linux. An application for obtaining task executions chronograms is presented as an example of application design under RT-Linux. Finally some measurements about context switching times are presented.

III. HOP-BY-HOP ENCRYPTION AND ITS INFLUENCE TO THE SOR

The standard Diffie-Hellman key exchange algorithm in order to securely create and distribute the shared keys among the neighbours using the created neighbour table .We need to select the best route depending on the real-time link conditions together in the least cost path.The protocol should use its own header structure and will copy the original sender and the receiver details in to the ability to route the packet to the optimum path also through the existing intermediate network devices such as normal routers and layer 3 switches as the packet contains an IP header. Encrypt the packet data and send it to the next hop SoR together with the original IP header and together with other SoR header information in order to identify the packet via the next hop SoR.

IV. ARCHITECTURE

The architecture of the proposed work consists of hop by hop tunnel in SoR based network:

A. End-to-end communication

In the end-to-end communication the connection between two parties will be established. In the second step the two parties will share the pairs of keys using public key architecture. After encryption the data can be sent through the selected network.The communication will be secured among the communication parties as the decrypting keys will to be known only by the communication parties. End-to-Encryption, in the proposed hop-by-hop encryption, the proposed protocol will encrypt the data while transmitting through the network. The encrypted tunnels will be created dynamically among the SoRs as the packets transmit through the network. When a packet is sending from client#1 to client#2, the packet will be sent in an encrypted tunnel in-between SoRs. Once SoR#1 receives the packet it will send the packet to SoR#2 through an encrypted tunnel in-between them.

After receiving the packet, SoR#2 will determine the most suitable path to forward the packet by analyzing its routing table. Then it will create a tunnel with SoR#3 or SoR#4 accordingly and forwards the packet.

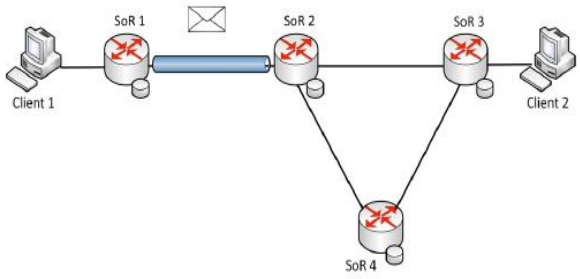

Fig 1. Hop –by – hop tunnel in SoR based network

In end-to-end encryption, first the end-to-end connection between the two communication parties will be established. Next, the two parties will securely share a key pair among each other using a public key architecture or any relevant method. Then the data will be sent through the selected path after encrypting using the shared keys. The communication will be secured among the communication parties as the decrypting keys will to be known only by the communication parties.

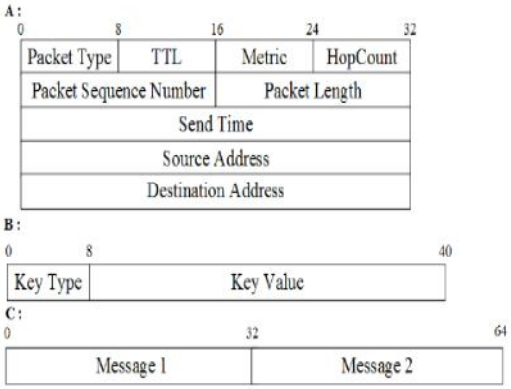

Fig 2 Packet Header structures used in the protocol

Basic protocol header structure used in the communications includes the control packets of the protocol.The header strucuture explain the Diffie-Hellman key exchange which will be stacked with the basic header when sending the key values.

V. PROPOSED WORK

In the proposed work the SoRs interfaces are up and the service oriented protocols will exchange the messages between the neighbouring nodes.If there is a failure in the neighbouring node it takes alternative path to transfer the data in the network. The exchange of keys between the nodes takes place and the SoRs will add and manage the generated key information in their own key table. The data packet encryption and decryption delay is reduced and is less than a 46.32 ***μs.*** The sensitive and confidential data will be protected by encrypting the data. The implemented secure data transmission protocol consisted of the following: It identifies the neighbours, per hop key exchange, maintain a distributed key table in every SoR. The proposed system encrypts and decrypts packets on arrival and departure to/from SoR.

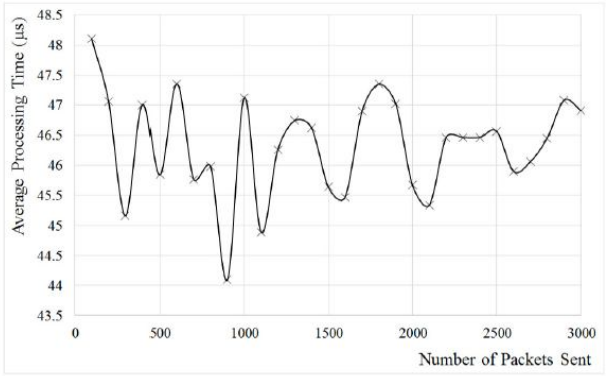

Fig3. Average Processing time of packets

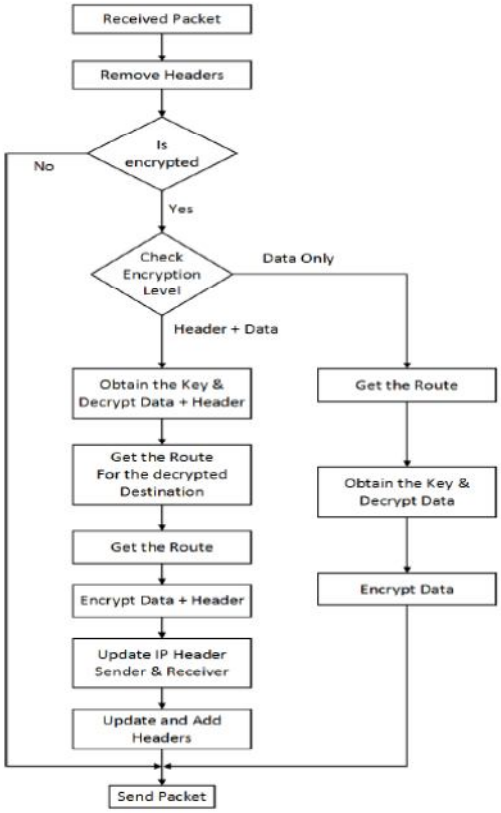

Fig 4. Flow chart for packet encryption process

VI. CONCLUSIONS

In this paper, a hop-by-hop protocol has been introduced and the data packets are transferred through the network. Since the data is encrypted the data is highly secure, data integrity is achieved. The issues and flaws of the existing system have been identified with the help of test results. Delay in the transfer of data packets is reduced and this is achieved with the help of test results. A processing delay of 50.32 µs is negligible and further can be reduced by high-end processing power and using advanced hardware architectures. The data encryption and decryption take less than a 46.32 µs. Enhanced features of Service Oriented Protocols can act fast enough by providing almost negligible processing delays for the haptic data packets. In the future the alternative way of reducing the delay in the transfer of packets and the security in the public networks can be achieved by using the most advanced hardware architectures. The new protocols will be implemented so that the data transfer is faster through the networks.

REFERENCES

[1] Rajitha Tennekoon,Janaka Wijekoon," Per Hop Data Encryption Protocol for Transmission of Motion Control Data Over Public Networks", March 2014.
[2] H King,K.Tadano "Preliminary protocol for interoperable telesugery", International Conference on Advanced Robotics,June 2009
[3] K Ikeuchi and J. Wijiekoon, "GPU-based multi-stream analyzer on application layer for service oriented router",IEEE 7th International symphosium on Embeeded,September 2013
[4] H.Sato,T. Yakoh "A Real Time communication mechanism for RT Linux",IEEE Industrial electronic society,2000
[5] P. Kihong, W. Wang "AFEC-Adaptive forward error correction protocol for end-to-end transport of real-time traffic",7th Interntaitonal Conference on Computer communications and Networks,October 1998
[6] H.Osman,M.Eid,P.Rubel,H.King,M.Koibuchi,"Evaluating ALPHAN:A communication protocol for haptic Interaction"March 2008
[7] A.Rovetta,R.Sala C. 2003. "the first experiement in the world of robotic telesurgery for laparascopy carried out by means of satellites networks and optical fibers networks on 7th july 1993"
[8] K. Takagiwa S. Ishida,H.Nishi, M.F, "SoR-Based Programmable Network For Future Software Defined Network", IEEE 37th Annual Computer Software and Application Conference.
[9] J. Wijekoon, R. Tennekoon,D. Harahap,"Service Oriented Router Module Implementation for ns-3"

