Proactive Authentication Mechanism to Secure Distance Vector Routing Protocol (RIPV2) by minimizing By-Pass Attacks

Rizwan Hassan[1], Saleem ullah[2 *], Gulfam Ahmed Umar[3]
[1]Department of Computer Science, The Islamia University of Bahawalpur, Pakistan
[2]Department of Computer Science & IT, Khwaja Fareed University of Engineering & IT, R.Y.Khan, Pakistan.
[3]Department of Computer Science, Ghazi University, Dera Ghazi Khan, Pakistan

ABSTRACT
Routing infrastructure is attacked to compromise the consistency of information transferred over the network, therefore, it is essential to secure network from insertion of illegal routing updates. In this research a proactive mechanism is proposed to secure routing protocols. This security mechanism works in a way that First secure authentication method for installing only trusted router is adopted so that installation of malicious routers into routing infrastructure is avoided. Secondly, use of secure cryptographic techniques for ensuring safest data transmission even on insecure transmission medium like internet. Cryptographic mechanism based on the use of hash function along with public key encryption method. Use of secure authentication method before acceptance of any incoming routing information or routing update promises better security. This research is focused on implementation of security mechanism including key exchange method, public key encryption along with router and message authentication for larger networks.

Key words:
Routing, RIP, SHA 512, Authentication, and Cryptography.

1. Introduction

Since security of routing infrastructure is extremely important. So, a proactive secure mechanism is required to overcome this problem. Routing devices and route information can be also attacked by intruders for purpose of intercepting sensitive information traversing over the network. Figure 1 Shows How data is transmitted through a Network and OSI Model in RIP routing mechanism. The shortest suitable path is adopted for transmission of packets from host A to host B.

Routing protocols [1-3] which provide better security mechanism protection the routing infrastructure. Sending path information and propagating of the packets through best suitable route are the key functions of a router. Routers can be attacked by which their main functions [4] can be compromised. Routing information and peering session can also come under attack and their information can be altered by unauthorized persons. Attacks, which can breach the security of hosts and servers, can also comprise the security of routers by different mechanisms [5-6] which can be overflowing the buffers, escalating the privileges and may be hacking the passwords.

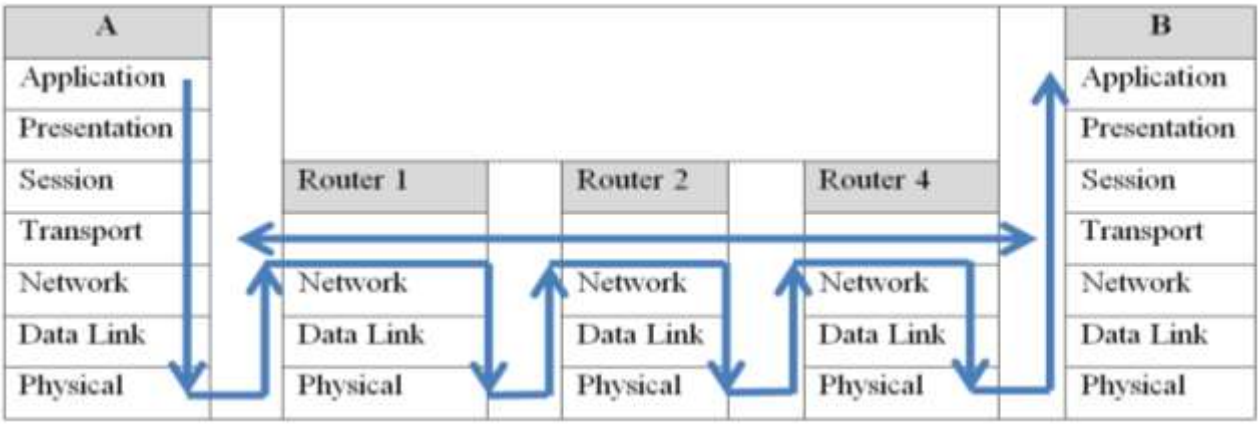

Fig. 1 RIP Routing Shows How data is routed through a Network and OSI Model

Manuscript received March 5, 2017
Manuscript revised March 20, 2017

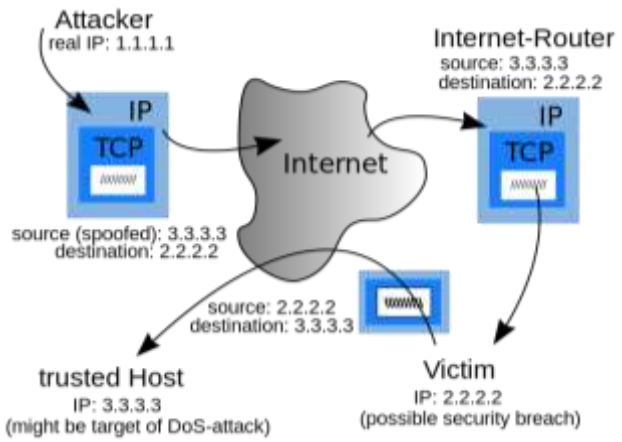

Fig. 2 IP Spoofing

Many of the research has been done on security in this area [7-10], however still require further improvement shown in figure 2.

Table 1 shows different types of attacks on routing protocols (category I to IX), threat level lower to higher.

Table 1: Attackers Classification

Attacker Strength	Communication Capability	Insider/ Outsider	Attacker Category	Attacker Goal on Route Integrity
Single Intruder	• Same as non-malicious node	Outsider	I	• Add self to route • Corrupt route
		Insider	II	• Corrupt route
	• Unlimited receive radius • Transmission radius same as non-malicious node	Outsider	III	• Add self to route • Corrupt route
		Insider	IV	• Corrupt route
	• No limitations (Dolev-Yao)	Outsider	V	• Add self to route • Corrupt route
		Insider	VI	• Corrupt route
Multiple Intruders (all intruder keys shared)	• Same as non-malicious node	Insider	VII	• Corrupt route
	• Unlimited receive radius • Transmission radius same as non-malicious node	Insider	VIII	• Corrupt route
	• No limitations (Dolev-Yao)	Insider	IX	• Corrupt route

Following chart shows the percentage cryptographic algorithm and their use in recent years in percentage.

2. Materials & Techniques

Proposed Model: New routers discovery means connection of incoming routers with the network for sharing of information. In this research only trusted nodes are allowed to be connected to an organization's network so that any information which is traversed on network should not use by any malicious node. Every router is allowed network connection after completion of necessary authentication process. New routers can be inserted into a network with static IP configuration of a router. Newly inducted router can participate in transmission of any routing update message or can also monitor the traffic traversing over the network. In this mechanism of static IP allocation of routers is carried out. Static IP of a router along with MAC address prevent bogus routers to be inserted into a network. Dynamic discovery process remains disabled in this mechanism. Authentication process is performed in two ways;

Firstly, IP address, MAC address, name and location of newly inducted router is inserted into main router for authentication process. Secondly, every router will be given a strong password with combination of alphanumeric keys for authentication process. For more secure environment password are randomly changed.

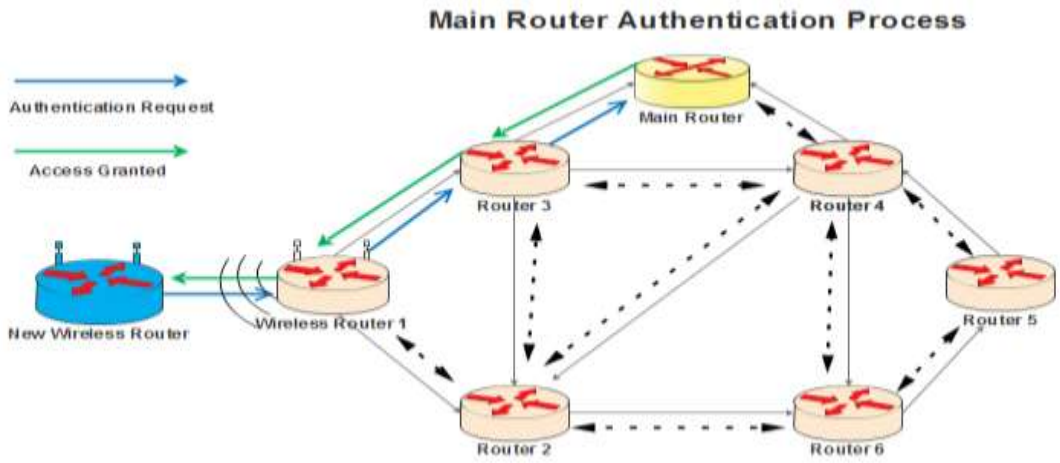

Fig. 3 New Router Authentication Process

Insertion of new routers using MAC address along with IP address provides more security to networking system then to ordinary automatic dynamic discovery process. As shown in Figure 3, the incoming router sends request for connectivity to a network by providing necessary password. The new router is then authenticated with help of IP address, MAC address and given password. During authentication process, the main router communicates rules, protocols and topology used with new router. With successful authentication the main router allows incoming router to connect to network for sending or receiving of updates message and other information. The same authentication process is repeated if the node is temporarily disconnected and again tries to connect with network.

As Shown in figure 3, figure 4 and figure 5, update messages can be transmitted in three different ways. One, the network router can receive updates from new router and does not share its updates. Second, the network router can send updates messages to new router and does not accept any updates from new router. Third, the network router can send and receive update messages from newly inducted router.

Fig. 4 Shows Routers Communication Process

In this way, communication can be secured more effectively. Static configuration of a router can have chances of IP spoofing. This risk of unlawful access to IP addresses can be secured with the use of Router's ID, Router's physical address and password protection. If any malicious router tries to connect to a network with the illegal IP addresses or passwords this mechanism denies illegal access to network. The MAC address is provided for the purposes that only trust routers should be connected to network.

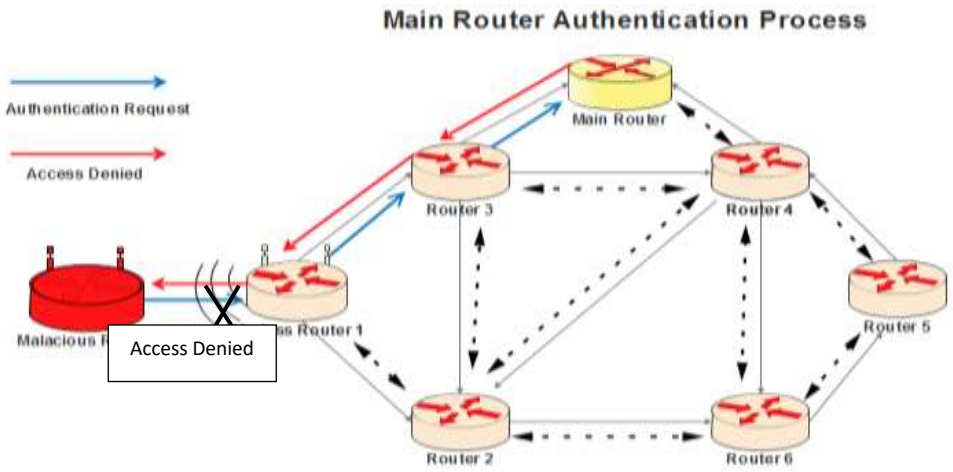

Fig. 5 Malicious Routers Connection Request

In Figure 5 a malicious router tries to connect to our network for any unlawful purpose. Our secure mechanism prevents any unauthorized router to access this network. As in our network all routers are manually configured and connected to share information. All routers are given unique Router ID and Password. When a router tries to access our network, it needs to provide Router ID, password and MAC address for authentication. If a malicious router obtains the Router ID and password by any means even then access can be denied. We propose a secure mechanism to configuring every router with its router ID, password and MAC address. Therefore the right router can be connected. In above case the access is denied to a malicious user.

Fig. 6 Trusted Router Successful Connection

Data Transmission: Figure 7 shows trusted router's successful connection to a network. After successful connection every router will give a unique Password to validate the authenticity of a routing update. It is guaranteed that data is received only from the trusted routers and the received information is reliable and correct. Data authentication is done between neighboring routers (Newly configured router and old network router) figure 6. Every router is given a secret key using public key encryption method to authenticate every incoming routing update message. Before transmission of any update message every router encrypts the message with the public key and attaches the obtained signature with routing update message as a part of it. Figure 7 shows the data transmission and message authentication process between neighboring routers.

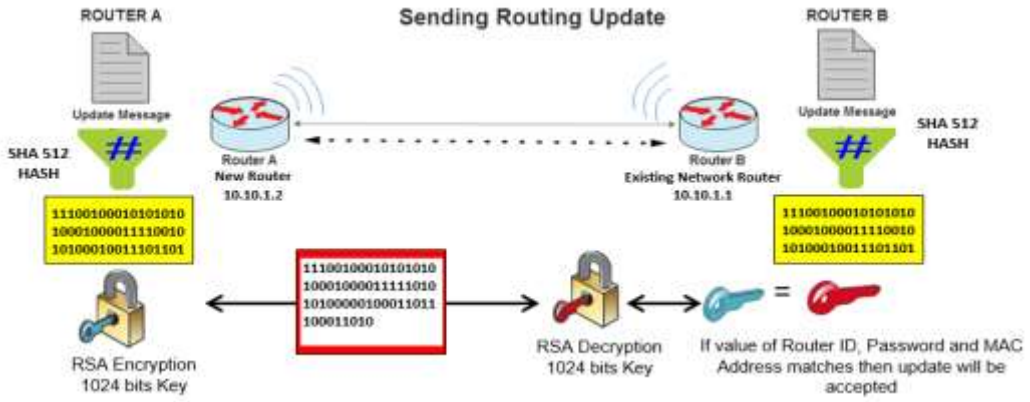

Fig. 7 Message Authentication Process

Router A is a newly configured router by static IP allocation method. New Router A is connected to an existing wireless network router using wireless connection. When Router A wants to send routing update message to Router B, it has to certify its authenticity and integrity of the update message. The message transmission is done in a way that a network router generates a set of public key and private key. Public key is sent to Router A for encryption and private key is saved within the network router (Router B) for decryption of message. Incoming message from Router A along with its Router ID, password and MAC address is processed through SHA 512 bits hash function to obtain hash value. This hash value is then encrypted using RSA 1024 bits Encryption algorithm with public key and message is sent to the network Router B. Message contain the Router ID, Password, Router Physical (MAC) Address, Source IP and Destination IP as shown in Figure 8.

Fig. 8 Message Format

Router B decrypts the message using RSA 1024 bits decryption method with private key and obtains hash value of Message, Router ID, Password and physical address. Router ID, password and physical address of new routers are stored on network router in form of hash value. The new router's Router ID, password and physical address are matched with its corresponding Network Router ID, password and physical address stored on neighboring network router. If hash value of Router ID, password and physical address matches with that stored in network router then this update message is accepted for updating of routing table otherwise rejected. In case of RIP protocol, routing update is sent after every 30 Seconds. Public key and private key can be generated using RSA is changed after every 30 minutes for encryption of decryption mechanism.

Our proposed algorithm i.e. table 2, works in a way, when a new router sends connection request, this request is sent to the main router for authentication. If new router is trusted then connection with the network is established. After successful connection, information between routers can be shared. Our proposed algorithm authenticates messages and updates shared within a network. In table 2. Step 1 it checks if the connection is successful then proceeds to step 2 otherwise process is finished. In Step 2 hash values of Message, Router ID, Password and Router MAC address are obtained using SHA 512 bits algorithm. In Step 3 the hash value of Message, Router ID, Password and Router MAC address are encrypted with RSA 1024 bits encryption method using public key. In Step 4 the encrypted message is sent over the network. In Step 5 the received message is decrypted with private key and hash values of Message, Router ID, Password and Router MAC address are obtained. In Step 6 comparison is done. If the hash value of Router ID, Password and Router MAC address matches with its corresponding Router ID, Password and Router MAC address stored in network then incoming message is accepted otherwise message is discarded. Detailed flow chart of the proposed algorithm is explained in figure 9.

Table 2: Proposed Algorithm for Secure Transmission of Routing Updates

Step 1	If New_Router_Connection="Successful" then
	Goto Step 2
	Else
	Goto Step 8

Step 2	Calculate Hash Value of Message, Router ID, Password and Router MAC address (M, RID, Pwd, RMAC) using SHA 512 bits algorithm
Step 3	Encrypt #Message, #Router ID, #Password and #Router MAC (#M, #RID, #Pwd, #RMAC) using RSA 1024 bits Encryption Method
Step 4	Send Encrypted Message / Routing Update
Step 5	Decrypt Received Message using RSA 1024 bits Decryption Method to obtain #Message, #Router ID, #Password and #Router MAC (#M, #RID, #Pwd, #RMAC)
Step 6	Compare If #RID = #Network_RID AND #Pwd = #Network_Pwd AND #RMAC = #Network_MAC then Goto Step 7 Else Discard Routing Update and Goto Step 8
Step 7	Accepted Message / Routing Update
Step 8	Finish

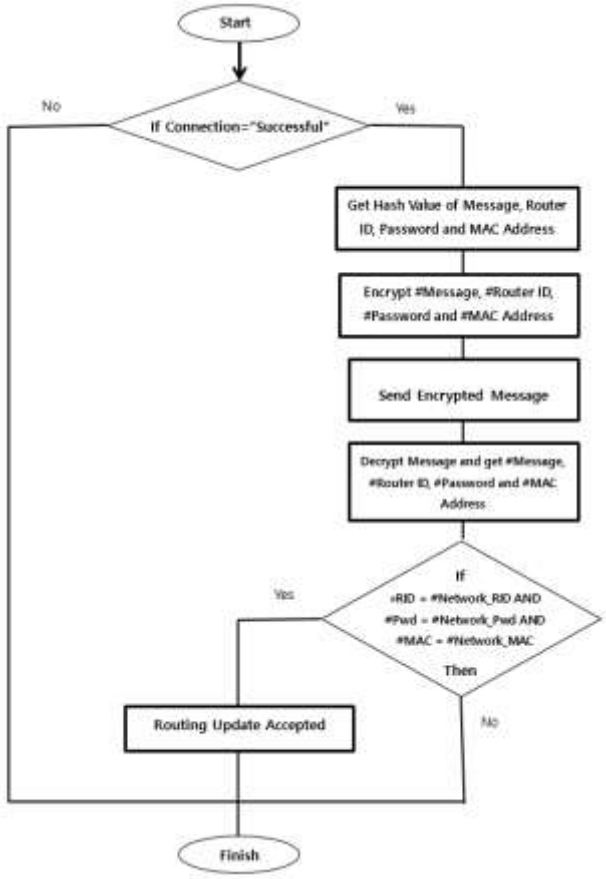

Fig. 9 Flow Chart for Secure Transmission of Update Message

3. Results & Discussion

Proposed Model Overview: Omnet++is used to claim the proposed algorithm. New routers can be connected to a network for sharing of information or sending messages and updates. Every new router will be manually configured for connectivity to our organization. On configuration of routers, Router ID and Passwords are assigned to them for authentication. After authentication connection will be established and exchange of information can take place over the enterprise Network. This newly proposed mechanism helps to authenticate all new incoming routers try to connect to our secure network. The connection request will be forwarded to main central router which can authenticate the incoming routers. Whenever request will be forwarded, it requires Router ID, Password and MAC address of the router. This Router ID, Password and MAC address are secured by getting hash value and then these Router ID, Password and MAC address are encrypted using RSA encryption.

Fig. 10 Router Connectivity Request

The request is forwarded to main router for authentication through wireless router, as shown in figure 10. The main router decrypts the Router ID, Password and MAC address and gets the hash value. Its corresponding is stored in configuration file of main router. Router ID, Password and MAC address of all routers of the network are stored for authentication. These values are hashed be placing into the file. Our network works on RIP (Routing Information Protocol) which is distance vector routing protocol which work for routers for transmission of information. RIP uses the hop count mechanism to find best route to the destination. Hope count means the number of routers that the message has to traverse till destination. Our network use RIP protocol which support only fifteen hop counts and usually sixteenth router is considered unreachable.

Connection Request: When successful connection is established between new router and network router they can exchange information. Information is then authenticated from new router for ensuring strong security of the network. The system is establishing the connection is not easy that an unauthorized person can be connected. However if the Router ID and password of legal router are compromised, the unauthorized person cannot get connection because the MAC Address of legal router is registered initially. Therefore the authorized person with authorized device can establish connection with our enterprise network.

Data Transmission: After having successful connection (figure 11) information can be exchanged with the help of different Router ID and password which are separately given for data transmission. If the same Router ID and Password are used then security may compromised.

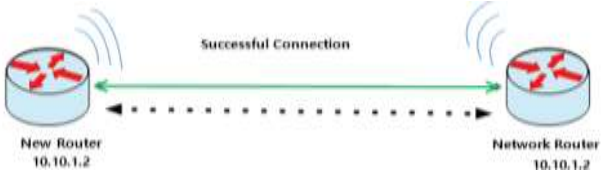

Fig. 11 Router Connectivity with Network

The information is sent to receiver in following way:-

Message will be forwarded after getting the hashed value. This hashed value will be encrypted with public key cryptography method. RSA is used to encrypt the message. Whenever connection will be established a pair of keys (Public Key and Private Key) will be generated from the network router. Public key will be sent to new router for encryption of information and private key will be kept secured with the network router for decryption of information. Sender will encrypt the message with public key and forward the message to network router. Information will be decrypted by the network router to get router id and password for authentication purpose. Network router maintains list of router ids and passwords of various routers with it for authenticating and validating information. Hashed value of Router id and password of new router will be matched with network router's set for accepting or rejecting the update message from new router. Figure 12 shows the above elaboration.

Message	Router ID	Password	Router MAC Address	Source IP	Destination IP
Hello	475c2e5c3a	R1$23%AFC@MR	08-3E-8E-59-B0-71	10.10.1.2	10.10.1.1

Fig. 12 Message Format

For secure transmission of a message following method is adopted so that message should be validated and verified. Hence it should be insured that the desired information has reached in its original format to its real destination and is trust worthy.

Network Simulation: On arrival of message at router 2, it authenticates the message shown in figure 13 before accepting incoming message.

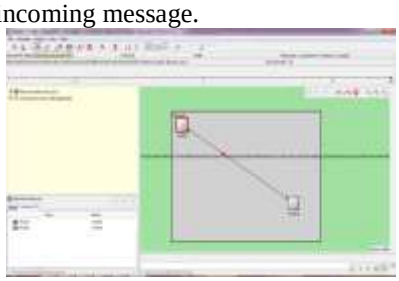

Fig. 13 Transmission of Cipher text from Router1 & Router 2.

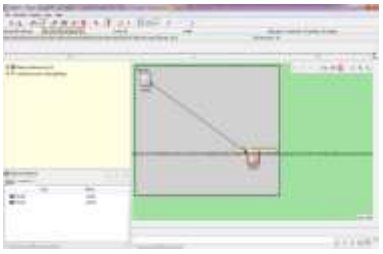

Fig. 14 Message Authentication Process.

The incoming message is then decrypted with private key and original hash value is received. The authentication process carry out matching the hash value of Router ID, Password and MAC address with their corresponding Router ID, Password and MAC address stored in network router, here in this case router2 is consider as network router. Before acceptance of message router 2 will carry out authentication, figure 14. After successful authentication the message is accepted.

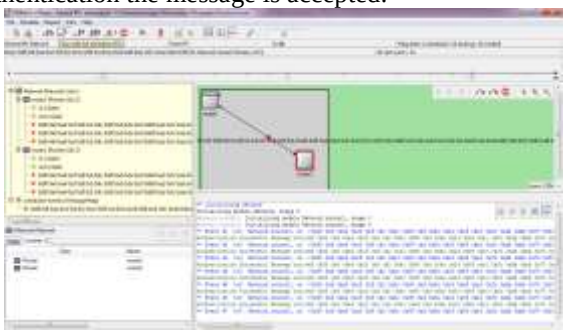

Fig. 15 Message Transmission from Router2 to Router1.

Router 2 can also send message to Router1 as shown in figure 15. Same hashing, encryption, decryption procedure will be performed by Router 2 and Router 1 as well as authentication process will be done by Router1 before accepting message from Router 2. This is how every time communication process between router 1 and router 2 will be carried out.

Figure 16 shows the transmission of message encryption message from Router 1 to Router 2 and Vice Versa in a time dependent fashion.

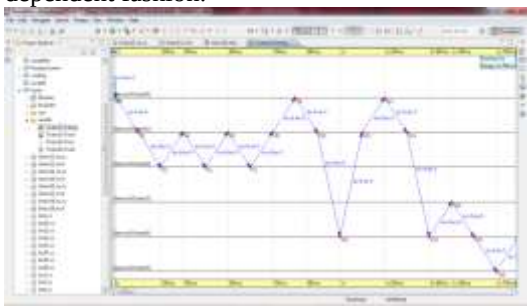

Fig. 16 Events Generation during Message Transmission

Routing updates are forwarded after establishing successful connections. We propose a security mechanism in a way that whenever a newly connected router sends routing update or information, it has to secure message value with hash function. SHA 512 is used for securing and authentication of a message. The message is then encrypted with public key encryption method. Public key is used for encryption of a message and for decryption private key is used. RSA 1024 bits encryption method is used for encryption and decryption of a message. Public key method ensures security of a message due to the fact that the private key is not shared with receiver. On receiving end password authentication is performed with its unique ID as well as physical address. If authentication of router is successful, it is assumed that the information is legal and sent by a trust router. Hence information or updates are accepted otherwise discarded.

4. Conclusion:

In this research a proactive mechanism for security of routing protocol is presented that prevents illegal attacks on routing infrastructure with more effectiveness. In this case routers cannot exchange information unless peering connections are established. Unlawful information can be sent along with packets. That's why node authentication is foremost important. Node authentication consists of secure connection mechanism, which is operated by network administrator. Entering only trusted nodes can secure network from illegal access and avoid malicious attacks on data or the data being silently observed. Dynamic routers discovery can cause unauthorized node to get illegal access to the network, hence static entry of routers is introduced. Static entry mechanism ensures that only trusted nodes are connected to the enterprise network. Every incoming router requires password authentication with its unique Router ID and its physical address. The authentication is process which is performed every time when router seeks connection with the network to be established.

References

[1] Anuj K. Gupta, Harsh Sadawarti, Anil K. Verma, Review of Various Routing Protocols for MANETs, International Journal of Information and Electronics Engineering, Vol. 1, No. 3, November 2011.

[2] Asma Adnane, Christophe Bidan, Rafael Timóteo de Sousa Júnior, Trust-based security for the OLSR routing protocol, Computer Communications 36 (2013) 1159–1171.

[3] Eduardo Feitosa, Eduardo Souto, Djamel H. Sadok, An orchestration approach for unwanted Internet traffic identification, Computer Networks 56 (2012) 2805–2831.

[4] Huaizhi Li, Zhenliu Chen, Xiangyang Qin, Chengdong Li, Hui Tan, Secure Routing in Wired Networks and Wireless Ad Hoc Networks, Department of Computer Science, University of Kentucky, April, 2002.

[5] Jiefeng (Terence) Chen, Roksana Boreli, Vijay Sivaraman, Improving the efficiency of anonymous routing for MANETs, Computer Communications 35 (2012) 619–627.

[6] Mathilde Arnaud, Véronique Cortier, Stéphanie Delaune, Modeling and verifying ad hoc routing protocols, Information and Computation 238 (2014) 30–67.

[7] M.S. Siddiqui, D. Montero, R. Serral-Gracià, X. Masip-Bruin, M. Yannuzzi, A survey on the recent efforts of the Internet Standardization Body for securing inter-domain routing , Computer Networks 80 (2015) 1–26.

[8] Neelam Khemariya, Ajay Khunteta, Krishna Kumar Joshi, A Robust Technique for Secure Routing Against Blackhole Attack in AODV Protocol for MANETs, International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013.

[9] Rushdi Hamamreh, Routing path authentication in link-state routing protocols, (2012).

[10] T.R. Andel, G. Back, A. Yasinsac, Automating the security analysis process of secure ad hoc routing protocols, Simulation Modeling Practice and Theory 19 (2011) 2032–2049.

Rizwan Hassan was born in Pakistan in 1981. He received BSc Computer Science, MSc Computer Science, MS Computer Science Degrees from Islamia University, Bahawalpur, Pakistan. He joined field of Education in 2005 as a Lecture at National University of Science and Technology (NUST), Pakistan. He has experience of teaching Computer Science at various renowned Colleges of Pakistan. Now he is doing as a Head of Computer Science Department at Jhelum College, Pakistan.

Saleem ullah is working as Assistant Professor with Khwaja Fareed University of Engineering & IT since Feb 2016. He completed his PhD degree from ChongQing University, China in 2012. He has almost 11 years of working experience in the field of IT. He is an active researcher in the field of Networks Congestion Control, Security.

Hafiz Gulfam Ahmad Umar was born in Pakistan in 1984. He received Ph.D and M.Sc degree in Computer Science from Chongqing University, China and Bahauddin Zakarya University Multan,Pakistan, in 2015 and 2005 respectively. From 2007 to 2014 he served as a lecturer in Agriculture University Faisalabad. Currently he is serving in department of Computer science, Ghazi University, D.G.Khan, Punjab, Pakistan. His research interest includes image encryption, intrusion detection systems, data mining, information security and cloud computing.