International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.3, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

CRACKING ALGORITHM FOR ACHIEVING SECURITY IN MULTIPLE ACCESS RELAY NETWORK UNDER FDI ATTACK

P.DHIVYA BHARATHI[1], P.SATHISHKUMAR[2]

[1]ME Student,Dept.of CSE,Anna University, Chennai,

[2]Assistant Professor, Dept. of CSE, Anna University, Chennai

Jayam College of Engineering and Technology, Dharmapuri DT, India

Article Received:13/05/2015 | Article Revised on:21/05/2015 | Article Accepted on:03/06/2015

ABSTRACT

In our day to day daily life many people facing problem due to the cause of the attack. To make the information in a hidden manner, and to overcome the attacker security is important. The sender sends information through the receiver through a relay. In multiple access relay network multiple sources send different data through the destination and may inject falsified data into the network. To detect malicious relays and to erase the data, tracing and parity bit is embedded in the source node. Tracing bit is used to identify errors in the source node and parity bit are used to correct the errors due to the fading and noise. In this paper, to detect the falsified data injection attack and to provide security from the attacker in the internet cracking algorithm is enhanced. Cracking algorithm is used to improve security and performance on the internet.

Keywords: Falsified data injection attack, cracking algorithm, Security, Performance.

1.1 INTRODUCTION

The network is used to transform the information from sender to receiver. While transforming information from sender to receiver security is needed. Security comes in all shapes and sizes, ranging from problems with software on a computer, to the integrity of messages and emails being sent on the Internet. Network security is a term to denote the security aspects attributed to the use of computer networks. This involves the protection of the integrity of the communication that are sent over the network. Network security consists of a set of rules adopted by the network. These network administrators are used to prevent and monitor third party user, user misuse and modification user. It involves authorization of data in the network. It covers both public and private because it is used for day to day business transaction process in a company. Network Security provides five services. The first, four services are message confidentiality, integrity, authentication and non-repudiation. Networks Beyond these four services are related to the message exchange using the network security and final services provides entity identification and authentication it is used to verify prior to access to the system resources.

The falsified data injection attack is one of the critical attack in the network. It may destroy the scheme (or) method used in the proposed system. This attack could not be filtered and verified. The user can send false reports containing some non-existing events to the destination. When the falsified data are injected through the destination, there is an exhaust out the limited energy and it is a waste of time when sending information from a sender to a destination. The false injection attack is more challenging for the mobility and hard to resist. To stop above the problem in the existing system to protect the network against FDI attack. In first step it limits the number of ICMP and SYN packet on router interface. In a second step it filters the private IP address using router access control lists and in the final step it applies ingress and egress filtering on all edge routers. The proposed method is affected by the falsified data injection attack because with this attack it can make the original data into a duplicate manner. By this process the scheme (or) method will get collapsed, it became the major critical to access the service. This generally occurs using a stolen account on a system with a large number of users that can be compromised and exploited. The compromised system can be loaded with number of cracking tools such as scanners and FDI data's. The FDI attack will become FDI header. The header software allows a large number of other systems and then the attacker can scan the large number of IP (or) MAC address blocks. The main goal of this process is to eliminate the FDI. When the attack occurs, the defense system ensures that due to packet loss and transmission only first SYN packet will get delayed and all other packets will receive the normal level of the client. As a result, it leads to security and performance improvement.

2.1 RELATED WORK

A lot of research work is going in the field of network security. Day by day new ideas are improving in this field. [1] In multiple access relay network, relay is the indirect communication for both sender and receiver. On the sender side, it has different data, relay nodes may combine all the data symbols received from different sources and these source data can be corrected by both parity and tracing bit. Tracing bit is used to detect malicious relays and parity bit are used to correct errors By correcting the error by using the two bits and then finally it shined through the single destination with error free These schemes are used to improve communication between sender and receiver. [2] Cooperative communication system with wireless communication to combat the unfriendly wireless environment. Some security issue may be rising. To overcome this Decode and forward strategy, this strategy is used for the security in cooperative wireless communication and it is trying to corrupt the communication by sending garbled signals. The cross layer scheme is used to trace and identify the adversarial relay nodes. This scheme is used in the physical layer and application layer. BECAN [4] (Bandwidth efficient, cooperative authentication) scheme used for filtering falsified data injection attack. This scheme can save time and energy. By saving energy and time the power will be increased and we can include more packet through the source node. [4] To detect the Byzantine modifications in network employing network coding. Multicast scheme is included in Byzantine modification based on network coding because it has different source data in the multicast scheme. For each packet they incorporate simple hash value. Sink node can detect the Byzantine modification with high probability and only for limited level. This application is designed to detect the Byzantine because only incomplete adversarial node is seen through the sink. When comparing through source node the third party may capture all, the entire message of the network coding and it has the transmission capacity. This approach may use in critical condition because it has different independent malicious nose. When receiving data from the destination node and data can be coded together in the independent adversarial packets. It provides much flexibility inconsistent between the detection and redundancy probabilities. The proportion of redundancy, the coding size and the amount of information about the network coding that is not observed by adversary. It is useful for monitoring during normal conditions. In cooperative communication for transmitting signal to receiver

requires more than one antenna. The size is limited is limited in the antenna, so they introduced cooperative communication.

3.1 EXISTING SYSTEM:

3.3.1 SECURITY IN MULTIPLE ACCESS RELAY NODE

The multiple sender source sends different data to a single receiver by multiple relays and then injected duplicate data into the network. To detect the harmful relay node tracing and parity bit is used. Tracing bit is used to identify malicious relay and parity bit are used to correct the incorrect once. When redundancy is included in both tracing and parity bit reliability will increase in parity bit and it decreases in tracing bit. As a result, it has less accurate security information. As a result, it has less error and maximize its throughput under FDI attack. But, FDI attack is the critical effect for using the method in the proposed system. To overcome this problem we are using cracking algorithm. By using code word the information is sent from sender to receiver through a relay. The source generates the independent packet each composed of (n, k+t) code word. The total redundancy is divided between tracing bit and parity bit. These both bits are used to detect malicious node in the relay. The relay may also receive the code word because it is the broadcast nature of the wireless medium. After decoding process it checks the error using a cyclic redundancy check, the set of relay without an error is called decoding set and finally the information is sent through the single destination

3.3.2 FDI ATTACK

An adversary aims to hack the reading of multiple relay and to mislead the user decision making process. One of the common adversarial attacks at the malicious relay node is to inject falsified data. The unknown relationship among the nodes makes it more vulnerable to duplicate data (falsified data injection attack). Whether the data packet is injected into the single node, as soon as it spread towards the whole network and then whole network get collapsed.

4.1 PROPOSED SYSTEM

4.1.1 CRACKING ALGORITHM

The main purpose of cracking algorithm is to eliminate FDI attack because FDI attack. In internet many people are accessing the service depend upon their purpose. When there are a number of users on the internet many people want to attack other system resources. When the user accesses the particular website, the website owner wants to make the website more popular than others. So, they want to attack the service of other websites. The user keeps on log on to a particular website more times and service provided by web server performance level becomes degraded. To overcome the performance problem this application maintains a status table. In the status table, i.e. register current user IP address and their status. If the particular IP address has been signed for a first time, it makes the status as genuine user. It marks as a normal user for 2, 3 and 4 times. For the fifth time it marks the particular IP address status as an attacker. The user wishes to server increase the time depend upon the application. After that the user cannot allow get the service of that particular website. The service is denied by that particular IP address. The server will monitor the user activities in the particular website, whether the user is using an own IP address or fake IP address. If the user is using a fake IP address the service will get denied.

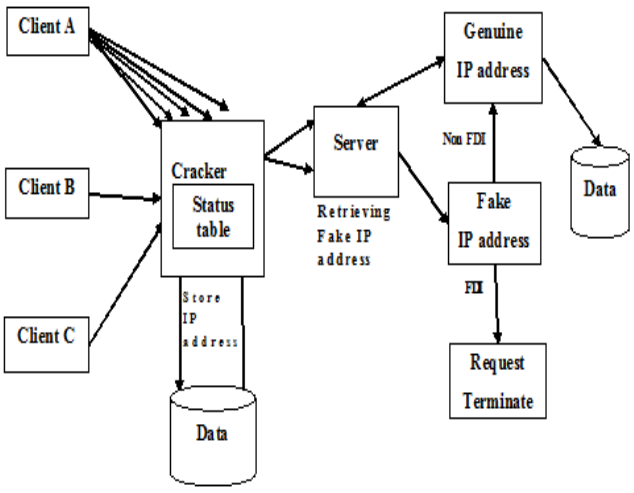


Fig 4.1 Block diagram of proposed system

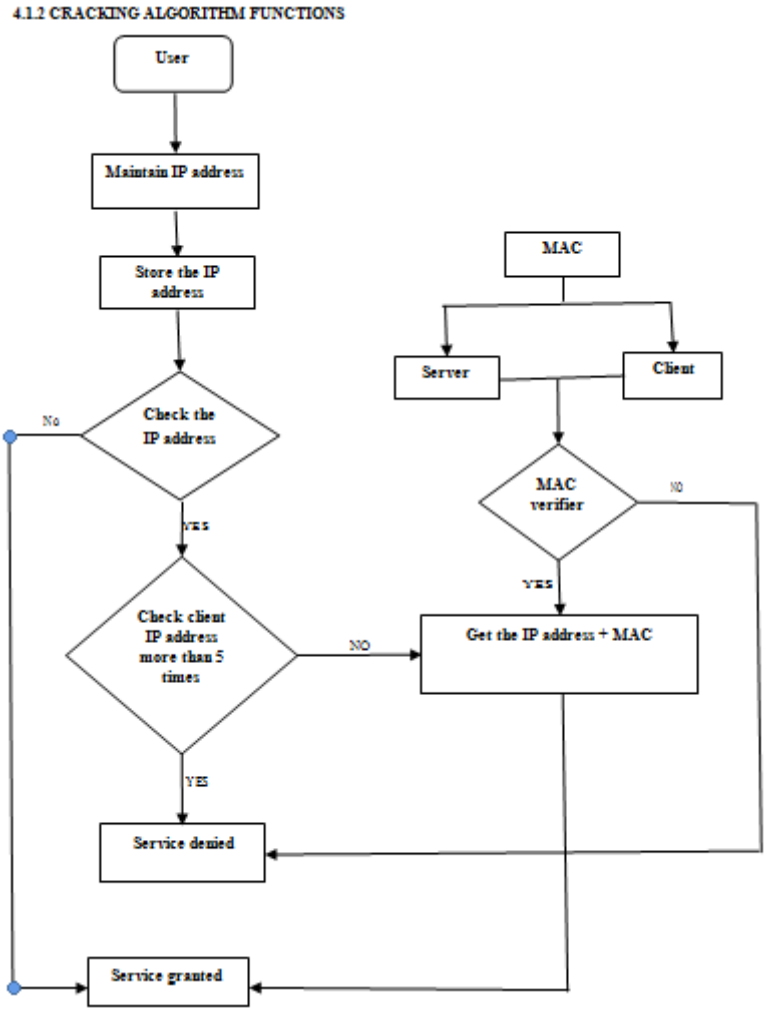


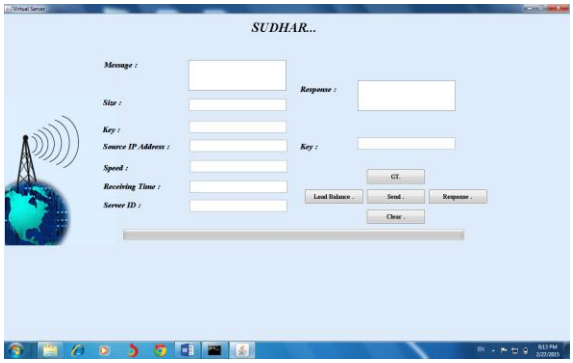
Fig 4.2 Cracking algorithm functions

The results of this paper are carried out by attackers and websites. The server updates each time user status, and at the same time the same information is provided through MAC address, time and IP address. Each time the user status will be updated by analyzing the website depends upon the IP address. When the new user entered into a particular website continuously the cracking algorithm will determine whether user is the FDI attacker or not. When the attacker is allowed to enter into the website, the status of the web server also calculated. Cracking algorithm is used to maintain user list and the attacker list by using the algorithm. When the attacker found the service access is denied and can't access the service to particular website. In this case, observer status is calculated. This is very useful for the user to determine efficiency of the proposed system.

In this client form request message, response message, encrypt key, decrypt key, bandwidth, size limit, maximum time as shown in this form. Here, port, id has to be entered in the client form, the port id secret form, message will be send through the router.

In client form, the second step is we have to set the key limit size and bandwidth as 512Kbps and then port id message will send through the encryption and decryption key and send the message through the router and automatic router form will be generated.

In this server form, the server will monitor the user activities in the particular website. When the user access the genuine IP address the service will be accesses else, whether user access the fake IP addresses the service will be denied.



In this router form the port id message will be transferred from the client side to the router form. Here message will be checked by using the load balance whether the message is fully loaded or not.

6.1 CONCULSION

In this paper, we proposed cracking algorithm for solving a continuous problem in the internet. The main aim of this paper is to eliminate the FDI (falsified data injection) attack because the FDI attack will cause damage for the proposed method. To degrade the server performance, the attacker will send large amount of unwanted information to the server. To overcome this problem, we propose a DDOS defense system. The main purpose of the defense system is used to improve performance in the webserver. Our system is easy to understand and it is easy to implement because it is transparent to both web server and the client.

REFERENCE

[1]. Taha A.Khalaf[1], Sang Wu Kim[2] and Alaa E. Abdel Hakim[3],"Tradeoff between reliability and security in multiple access relay networks under falsified data injection attack," March 3,2014.

[2]. Yinian mao[1] and min wu[2],"Tracing malicious relays in cooperative wireless communication,"Vol 2, June 2007.

[3]. Nicholas laneman[1], David N.C. Tse[2] and Gregory A.L.Wornell[3],"Cooperative diversity in wireless networks,"IEEE December 12, 2004.

[4]. Chitra.V, Hameetha begum, Ramya.M and Udhaya,"Filtering false data injection using the beacon scheme in sensor networks, "May 2014.

[5]. Tracey Ho[1], Benleong[2], Ralf koetter[3], Muriel medard[4] and David R.Karger[5],"Byzantine modification detection in multicast networks with random network coding," IEEE Trans. Inf. Theory, Vol 54, No.6, pp. 2798-2803, June 2008.

[6]. Nosratinia[1], T.E. Hunter[2] and A. Hedayat[3],"Cooperative communication in wireless network,"IEEE common. Mag, Vol 42, No.10, pp. 74-80, Oct 2004.

[7]. S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, et al., "Resilient network coding in the presence of Byzantine adversaries," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2596-2603, Jun. 2008.

[8]. Y. Chen, S. Kishore, and J. Li, "Wireless diversity through network coding," in Proc. IEEE WCNC, Las Vegas, NV, USA, Apr. 2006, pp. 1681-1686.

[9]. C. Hazel and P. Dupraz, "Joint network-channel coding for the multiple access relay channel," in Proc. 3rd Annu. IEEE Commun. Soc. Sensored Hoc Commun.Netw. Reston, VA, USA, Sep. 2006, pp. 817-822.

[10]. F. Zhao, T. Kalkert, M. Medard, and K. J. Han, "Signatures for content distribution with network coding," in Proc. IEEE Int. Symp. Inf. Theory, Nice, France, Jun. 2007, pp. 556-560.

[11]. B. Kaliski, "The MD2 message-digest algorithm," RSA, Lab., Toronto, ON, Canada, Tech. Rep. RFC 1319, Apr. 1992.

[12]. S. Dane, H. T. Sencar, and N. Memon, "Towards an Information Theory of Large Networks: An Achievable Rate Region," in Proc. 41st annual. CISS, Baltimore, MD, USA, Mar. 2007, pp. 895-899.

[13]. Andrew Sendonaris, ElzaErkip and Behnaam, "Increasing uplink capacity via user Cooperation Diversity, "ISIT 1998, Cambridge, M.A, USA.

[14]. AradhanaNarula, Mitchell D.Trott and Gregory W.Wornell, "Performance limits of coded diversity methods for transmitter antenna arrays,"IEEE, November 1999.

[15]. LizhongZheng and David N.C.Tse,"Diversity and multiplexing: A fundamental tradeoff in multiple antenna channels, "member IEEE, May 2003.

[16]. Michael just par and Martin Vetterli,"On the asymptotic capacity of Gaussian relay networks, "July 2002.

[17]. Javier garclafrias and Weizhong,"Approaching Shannon performance by iterative decoding of linear codes with low density generator matrix, "June 2003.

[18]. Rudolf Allowed, Nicki and shoo yen Robert Li,"Network information flow", IEEE, July 2000.

[19]. Nicholas. J lineman and Gregory W. Wornell,"Distributed space, time coded protocols for exploiting cooperative diversity in wireless network,"IEEE, October 2003.

[20]. Mohammed Janani, AhmadrezaHedayat, ToddE. hunter and Aria nosratinia,"Coded cooperation in wireless communications: Space time transmission and iterative decoding,"IEEE, Feb 2004.