PROFICIENT AND SECURE ROUTING APPROACH FOR WIRELESS MESH NETWORK

Shilpa
Department of Computer Science & Engineering
PURCITM, Mohali

Kamaljeet Kaur Mangat
Department of Computer Science & Engineering
PURCITM, Mohali

***Abstract*—Wireless mesh network has served as backbone for establishment of several upcoming technologies. It is possible owning to self healing, auto configuration nature of these networks. On one hand it offers an ease for compatibility, availability, feasibility however on other hand these networks are prone to various security attacks. These security attacks can sabotage the communication between sender and receiver . A need of algorithm that can prevent the network from security attacks such as DoS attack. The proposed work implements Hash RSA algorithm with help of Genetic algorithm to mitigate DoS attack. The network parameters used are throughput, end to end delay and jitter to evaluate the performance of algorithm under different scenarios.**

Keywords- Dos attack, Encryption, Genetic Algorithm,Hash RSA , Network Security

I. INTRODUCTION

Wireless mesh networks (WMNs) are comprised of mesh routers (i.e. nodes) and mesh clients (i.e. users).Mesh routers defines the backbone of wireless network and mesh clients connect on to the routers [10]. Mesh clients make access to the network through mesh routers. They can directly connect i.e. mesh with each other [9]. WMN has served as backbone for establishment of several upcoming technologies because of their self-healing and auto configuration nature [9]. Security is one of the major concern in WMN as these networks are prone to various attacks such as Denial of Service (DoS), user related (spoofing, IP addressing issues) and black hole attacks. There exist high need to secure the network from various attacks for deployment and its use in real life scenarios[9]. For quick deployment of WMN, switches acting as nodes are not moveable and have numerous radio handsets, which permit them to discuss quickly with more than one neighbor while utilizing the diverse channels[7][8].

Denial of service (DoS) attacks has now become a serious threat to current networks[17][18] . Earlier DoS attacks were like games played via underground attackers. As an example, an offender may wish to get control of an IRC channel via playing DoS attacks against the channel owner[19][20]. Now it has become a serious issue. Various mitigation techniques and defense mechanism are proposed for DoS attack. Some of these techniques degrade the network performance by consuming the available resources. There is a need to secure network from these attacks.

RSA was created by Rivest-Shamir-Aldman .It is an asymmetric algorithm and most recognizable which is used for generation of public ,private key and encryption. For enhancing the security ,data passed to the RSA algorithm is hashed . Digital signatures are included and public key cryptography to further enhance the security[23].

In this paper, a proficient and secure routing approach is developed, that protect the network. The proposed approach simulates the Hash RSA algorithm to protect the network from DoS attack. Furthermore it improves the security of the Hash RSA with the help of the genetic algorithm optimization. The simulation of the network has been done using MATLAB simulator. The algorithm is evaluated on the basis of performance parameters such as end to end delay, throughput and jitter under different scenarios.

II. LITERATURE REVIEW

Transmission power or scope of switches can be chosen from downplayed set of conceivable extents [6]. The Node solicitation of hosts is gathered per hub; these hosts are in the transmission scope of the hub. The future model can be utilized independently to determination clients' presentation: every switch is substituted by a host with an interest [4].The programmer can work the data and draw in every one of the payloads and misappropriations the UAV's because of which there are parcel of dangers of dropping bundles [5] by the programmer or outsider. The programmer can misfortune the course and produce the fake copy course and makes the possibility of every bundle to go on that fake/copy course [4]. Programmer can create the different fake Traffic duplicates of the Unmanned Aerial vehicle to build the parcel above which diminishments the throughput of the system and reductions the system lifetime which influences the course revelation delay in the system [6].

A PA-SHWMP, which joins new element standing instrument taking into account subject rationale and vulnerability with the multi level security innovation. Dad SHWMP can shield to the interior assaults brought on by bargained hubs and fulfill more grounded security and protection insurance [9]. To finish high-limit execution, the numeral of cross section switches and the quantity of gets to must be precisely picked. It likewise uncovered that a WMN can fulfill the same asymptotic yield limit as that of a half and half impromptu system by showing just a little number of interlocks switches [8]. This paper gifts equipped calculations to actualize multicast declaration in wormhole steered direct systems, by abusing the belonging of the changing over innovation. Least time multicast calculations are possible for n-dimensional lattices and hyper 3D shapes that utilization measurement requested overwhelming of unicast messages [7].

The Secure HWMP (SHWMP), to provide authenticity and integrity of HWMP routing messages and stop unauthorized manipulation of changeable fields inside the routing information elements .To attain this, they use the Merkle tree approach to authenticate changeable info and radially symmetric key cryptography to defend the mutable field. Simulation results illustrate that the SHWMP provides high packet delivery ratio with little increase in end-to-end delay, path acquisition delay, in addition to regulate byte overhead. Though, the proposed protocol is prone to the attacks caused by the inner legitimate mesh routers [12].

Denial of Service (DoS) attacks has proved to be a heavy and permanent threat to users, organizations, [14][18]. The primary goal of these attacks is to intercept access to a specific resource sort of a web server [4]. An outsized range of defences against DoS attacks have been projected in the literature, however none of them provides reliable protection. There will always be invariably vulnerable hosts in the web to be used as sources of attack traffic. It is merely not possible to expect all existing hosts within the web to be protected to a tolerable degree (in July 2005 it was estimated that there were approximately 350,000,000 hosts in the Internet [16]). Additionally , it is very hard to reliably acknowledge and filter solely attack traffic while not causing any collateral damage to legitimate traffic.

A DoS attack can be defined out either as a flooding or a logic attack [15]. A flooding DoS attack relies on brute force. Real-looking however extraneous data is sent as much as feasible to a victim. As a result, bandwidth of network is dissipated , disk space is filled with extraneous data (such as spam e-mail, junk files, and intentional error messages), fixed size data structures within the host software area unit filled with imitative information, or processing power is spent for useless purposes[13]. To amplify the consequences, DoS attacks can be worked in a coordinated manner from many sources at the identical time (Distributed DoS, DDoS). A logic DoS attack is built on an intelligent exploitation of vulnerabilities with in the target. As an example, a skillfully constructed fragmented Internet Protocol (IP) datagram might crash a system attributable to a heavy fault with in the operating system (OS) software[11]. Another example of a logic attack is to use missing authentication needs by injecting imitative routing information to intercept traffic from reaching a victim's network.

III. PROPOSED WORK

A high need of security in routing protocols for the well-organized routing due to which there will be less unplanned of packet drops and high delivery of packets with less delay from source to destination [5]. Routing protocols need to be secured for the efficient routing for efficient delivery of packets.. The DoS attacks and there protection is one of the major concerns which needs to be solved.A need of algorithm that is efficient and quick to prevent against these attacks.

IV. PROPOSED SOLUTION

In the proposed work the DoS attack is eliminated by black listing of malicious node after detection of node as malicious and non malicious. The figure below gives an idea of the elimination of malicious nodes after the identification of malicious nodes by using the Hash RSA algorithm and improving and optimizing the key generation process of Hash RSA algorithm with the help of Genetic Algorithm.

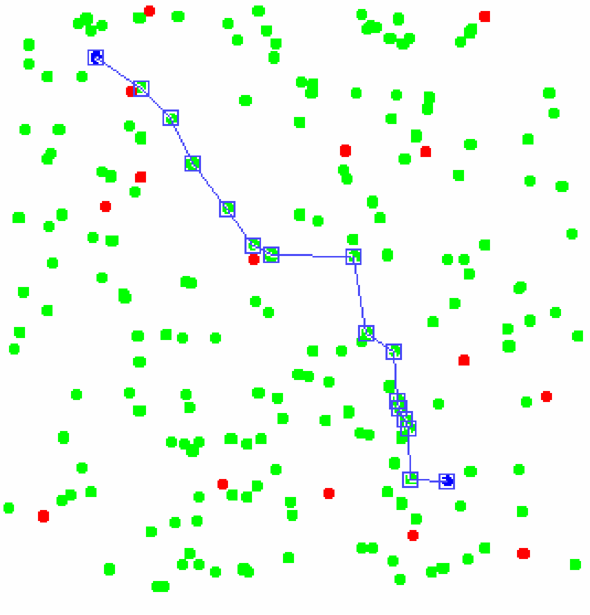

Fig.4.1 Simulation of the system

The discussion of the simulation starts form the initial steps of network setup involving the node deployment and the network basic setup like location tables and distance table for routing. After the initial setup the nodes are used to simulate the routing in the first place for the normal scenario. The network is given a source and a destination as input and the routing of the packets start from the source to the sink. Then the network simulation of the DOS attack is done in which the some nodes are given the properties of the attacker. With the use of Hash RSA algorithm the identification of the attacker is done

The request from the normal nodes comes; the normal nodes are able to verify their identity by the use to of private key they uses to authenticate them. While on the other hand the malicious nodes are not able to do this nut they continually send the request for the packets. The failure of the nodes in authentication process make them invalid and black listed in the future premises, Some brute force attack are also assumed in the network by which the malicious node can break the Hash RSA algorithm encryption. So it requires the use of genetic algorithm for optimization in order to improve the results. The below fig 4.2 denotes the steps involved in implementation of algorithm.

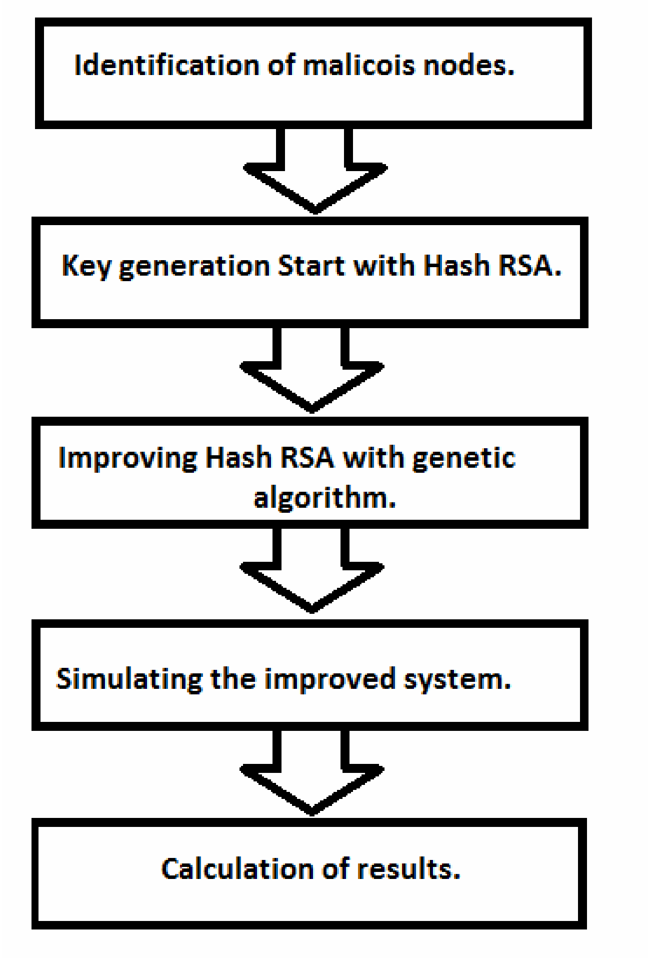
Identification of malicois nodes.
Key generation Start with Hash RSA.
Improving Hash RSA with genetic algorithm.
Simulating the improved system.
Calculation of results.

Fig 4.2 . Block diagram of Methodology

V. SIMULATION RESULTS

The first evolutionary-based technique provided in the literature was the genetic algorithm (GA). GA was developed built on the Darwinian principle of the 'survival of the fittest' and the natural predefined task of evolution through reproduction,cross over. [3] Based on its demonstrated ability to reach the near to optimum solutions to large problems, the GA technique has been applied in many applications in science and engineering. Despite their benefits, GA may require long processing time for a near optimum solution to evolve. Also, not all problems lend themselves well to a solution with GA

Fig.5.1 shows the graph of the average fitness of the populations of prime numbers used for the improvement of the Hash RSA algorithm used in the simulation of the DOS attack protection . The initial population has the value as low as the zero level ,with increase in iteration the level of fitness increases as depicted and Final fitness achieved is much better from the start which proves the utility of the genetic algorithm used.

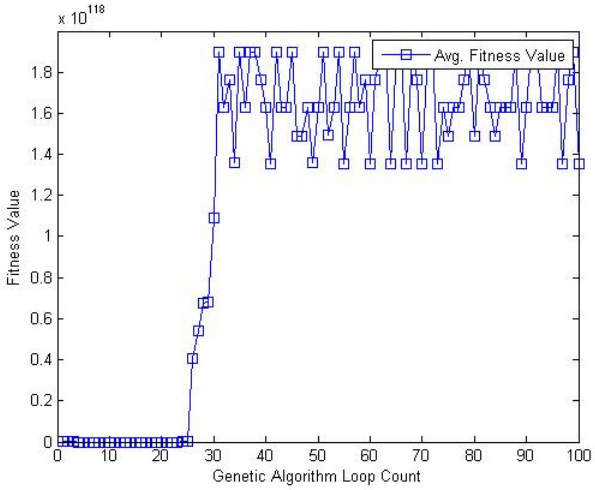

Fig 5.1 Fitness value over Genetic Algorithm iteration

Fig 5.2 shows the graph between the Throughput and the number of rounds. This is a cumulative graph in which the various rounds are simulated and the result achieved are added.

Throughput=Number of packet/Time taken

The throughput of the system is decreased to choke during the attack. As evident from the graph the throughput improves from the simulation of attack and the packet per second increase due to the use of Hash RSA algorithm. Throughput is further improved as the Hash RSA is optimized with the help of Genetic Algorithm.

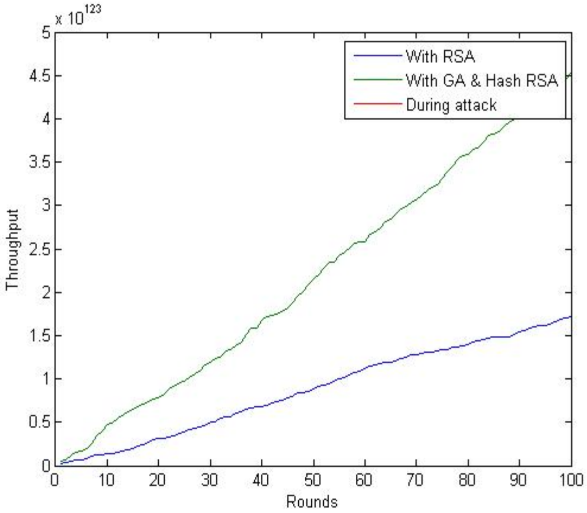

Fig 5.2. Throughput Comparison

Fig 5.3 represents the results of End to End Delay of the system.The end to end delay can be defined as the time utilized in taking the packet across the network.It is a one way delay for the packet to be transmitted from source to destination.. With the use of Hash RSA the packets start to route again and the malicious nodes are black listed. Due to the avoidance in malicious nodes the delay of packet also decreases with the help of Hash RSA and Genetic Algorithm.

Average End to End Delay=1/Throughput

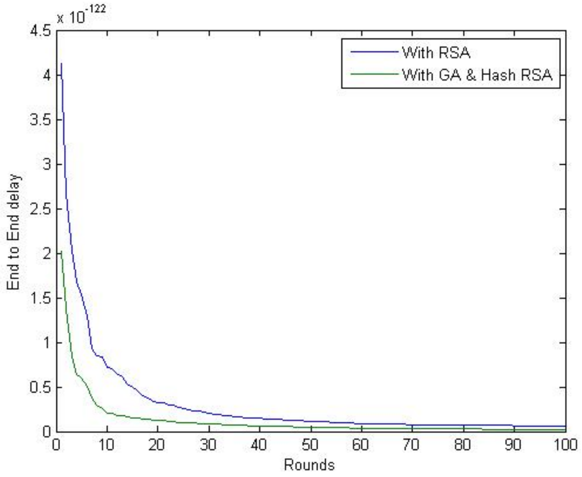

Fig 5.3. End to End Delay

Fig. 5.4 represents the jitter in the network. The jitter is outlined as a variation within the delay of received packets.Source transmits packets during a continuous stream and areas them equally.Due to the network congestion and improper queuing the delay between packets vary instead of remaining constant.The jitter is like end to end delay that losses its value during the attack due to the unavailability of the packets.As is evident from the graph jitter improves with the use of Hash RSA and further more by the use Genetic Algorithm

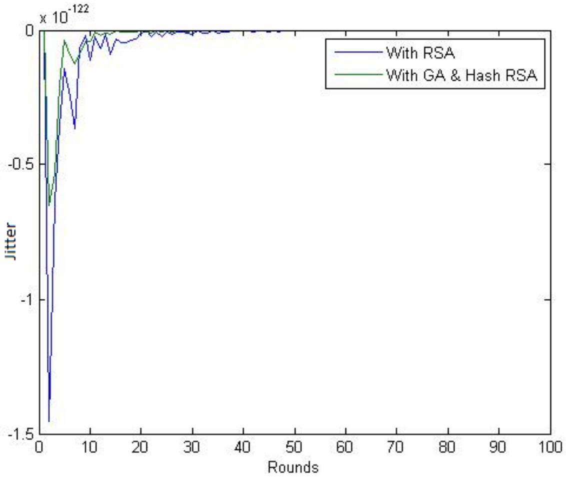

Fig 5.4 Comparison of Jitter of RSA with GA over Hash RSA

The algorithm has been implemented and validated under different network scenarios.Three simulation scenarios have been designed containing the varying number of nodes . The description of these scenarios is given as

Scenario-1: 150
Scenario-2: 200
Scenario-3: 250

Table 5.1:Performance of Hash RSA algorithm optimized with genetic algorithm in networks of variable size

Scenarios	Scenario 1	Scenario 2	Scenario 2
Throughput	2.462	2.483	2.917
End to End Delay	1.514	3.77	3.86
Jitter	-5.9	-4.8	-5.7

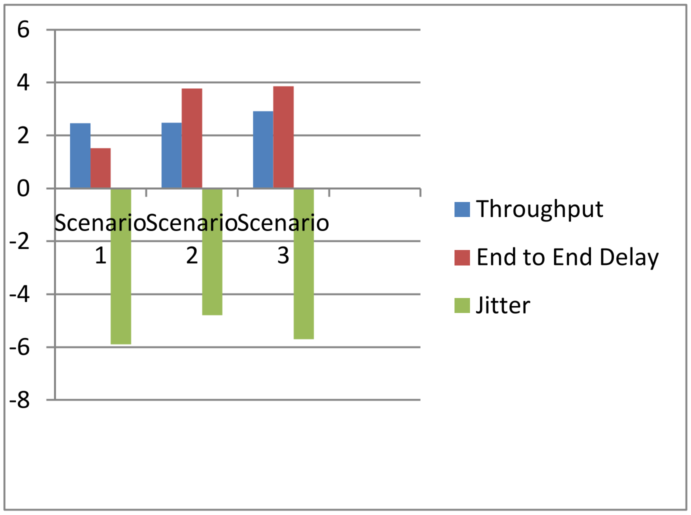

Fig 5.1 Performance of algorithm under different scenarios

VI.CONCLUSION AND FUTURE SCOPE

WMN is now a day's providing an extensive support for IP services and upcoming technologies. Security is one of the challenging issue still exist in wireless mesh network. There is a high need to protect the network from attacks and making it furthermore reliable to form the backbone of many existing infrastructure.

The work done in this paper shows the elimination of malicious nodes with the help of Hash RSA algorithm optimized with the use of genetic algorithm. The simulation of the network was done in MATLAB with the effect during the DoS attack. We identified the malicious nodes and then black listed them during the routing. Genetic algorithm was used in improving the key generation process of the Hash RSA algorithm. The results show significant improvement with the use of Hash RSA optimized with genetic algorithm . The performance was analyzed and checked on various parameters like throughput, jitter and end to end delay. The performance of Hash RSA optimized with genetic algorithm is validated under different scenarios in terms of variable number of nodes. Throughput of algorithm increases with increase in number of nodes. Whereas end to end delay varied less in nature. The slight increase is due to congestion in network. Jitter value increases by increase in nodes. The high negative value portrays jitter has improved .Due to congestion in network there is slight variation in delay of packet. The algorithm performs better in terms of all parameters. It provides much greater performance and handles the security of network

Security feature in network has attracted many researchers. In the future scope the implementation of algorithm can be applied in various application scenarios such as to relay the communication between UAV, deployment of IP services. Thus it will help in making wireless network furthermore reliable.

REFERENCES

[1] Sbeiti, Mohamad, et al. "PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks."IEEE Transaction, 2015.

[2] Y. Zhang and Y. Fang, "ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks," IEEE Journal on Selected Areas in Communications, vol. 24, No. 10, 2006.

[3] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of Wireless Communication Technologies for Public Safety," IEEE Communications Surveys Tutorials, vol. 16, No. 2, 2014.

[4] Sheng, Liu, et al. "Research on optimization efficiency of Genetic Algorithms." Systems and Control in Aerospace and Astronautics, 2008. ISSCAA 2008. 2nd International Symposium on. IEEE, 2008.

[5] Crosbie, Mark, and Gene Spaffor, "Applying Genetic Programming to Intrusion Detection." In Proceedings of AAAI Fall Symposium on Genetic Programming, Cambridge, Massachusetts , 1995, pp. 1-8.

[6] Kerpez, Kenneth J. "Coaxial cable passive mesh networks."Communications, IEEE Transactions ,vol 45,pp. 937-947,1997.

[7] McKinley, Philip K., et al. "Unicast-based multicast communication in wormhole-routed networks." Parallel and Distributed Systems, IEEE Transactions ,vol.5 no.12 , pp.1252-1265,1994.

[8] Zhou, Ping, Xudong Wang, and Ramesh Rao. "Asymptotic capacity of infrastructure wireless mesh networks." Mobile Computing, IEEE Transactions ,vol.7 ,pp. 1011-1024,2008.

[9] Lin, Hui, et al. "PA-SHWMP: a privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11 s wireless mesh networks." EURASIP Journal on Wireless Communications and Networking, 2012.

[10] M. Richtel. "Yahoo Attributes a Lengthy Service Failure to an Attack," in NY Times Online Article available at: http://www.nytimes.com/library/tech/00/02/biztech/articles/08yahoo.html, February 8, 2000.

[11] D. McGuire and B. Krebs. "Attack on Internet Called Largest Ever," in Washington Post Online Article available at: http://www.washingtonpost.com/ac2/wpdyn?pagename=article&contentId=A828-2002Oct22&notFound=true, October 22, 2002.

[12] E. Skoudis. CounterHack. A Step-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall, Upper Saddle River, NJ, 2002.

[13] A. Belenky and N. Ansari. "On IP Traceback," in IEEE Communications Magazine. Vol. 41, Issue 7, July 2003, pp. 142-153.

[14] J. F. Kurose and K. W. Ross. Computer Networking. A Top-Down Approach Featuring the Internet, 2nd Edition. Addison Wesley, Boston, MA, 2003.

[15] R. K. C. Chang. “Defending against flooding-based distributed denial-of-service attacks: a tutorial,” in IEEE Communications Magazine. Vol. 40, Issue 10, October 2002, pp. 42-51.

[16] P. Ferguson and D. Senie. “RFC 2267 – Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.” January 1998.

[17] J. Postel. “RFC 793: Transmission Control Protocol,” September 1981.

[18] CERT® Advisory CA-1999-17 Denial-of-Service Tools. Available at: http://www.cert.org/advisories/CA-1999-17.html. December 1999.

[19] Packet Storm Security. Online security reference website available at: http://packetstormsecurity.org/

[20] J. Lemon. “Resisting SYN flood DoS attacks with a SYN cache”, in Proceedings of USENIX BSDCon, February 11-14, 2002, pp. 89-98.