Enhanced Secure Hash based Client Puzzle approach to defend against Cyber Attacks

M.Uma
Ph.D Research Scholar
Department of Computer Science
Avinashilingam Institute for Home Science and Higher Education for Women
Coimbatore -641043

Dr.G.Padmavathi
Professor and Head
Department of Computer Science
Avinashilingam Institute for Home Science and Higher Education for Women
Coimbatore -641043

ABSTRACT

Game theory is a widely used technique for network security. As technology grows, the cyber worlds are more vulnerable to unknown cyber attacks. There are many cyber attack detection methods available for known attacks; however, efficient methods are essential to detect the unknown cyber attacks. In this research work, an enhanced hash based game theory approach is introduced to defend against cyber attacks. The proposed method is tested in a simulated environment and the method is evaluated using the performance metrics like Throughput, End to end delay, Packet delivery ratio, routing overhead, energy consumption and latency.

KEYWORDS: Game theory, Client puzzle, Hash Chain, Cyber Attacks, Elliptic curve cryptography

1. INTRODUCTION

Passive attack is a process of hacking the communicated data without giving any alerts [1]. There will not be any mess up in the network. There are still more challenges in detecting the passive attacks. Traffic monitoring, Eavesdropping, Traffic analysis and Syn flooding are the termed as passive attacks [2] [3]. Though many methods are available some more efficient techniques are still needed to handle unknown cyber attacks.

Now a days, as technology grows the vulnerability also higher for hacking the data or information. In the year 2009, in cyber leap year summit it is suggested that game theory plays a

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

major role in network security. Game theory is nothing but a security game played by the attacker and the defender [12]. In the game theory approach the attacker and the defender can play a game as single stage, two player and non-zero sum games [13]. The existing game theory approach for network security problem and the author [14] classifying the solution into two categories namely attack-defense analysis and security measurement. Moreover the game theory based solution for network security is commonly classified [15] into two categories namely cooperative game models and non-cooperative game models. In the game theory approach consists of four basic elements say Players, Actions, Payoff and Strategies. The games applied in game theory approach are broadly classified into three various methods and they are based on the number of stages, Based on perfect information or not and Based on complete information or not. The classification of game theory applications in network security, the notions are System, Attacker, Attack target, Intrusion Detection System, Virtual sensor and Defender.

Client puzzle protocol (CPP) is an algorithm [16] which is used to harden the process of hacking the network resources. The basic concept of this CPP is requesting all the clients which are connected to the server to solve the mathematical puzzle in a given time to establish a connection. Each client will send the solution to the server after solving the puzzle. After that, the server will verify the solution and will decide to establish a connection or to drop a connection.

Client puzzle protocol plays a vital role in network security, developed in the year 1992 against email spam. Client puzzle is basically based on hash function; hardly one or two hash function is required to generate a puzzle [6]. Nash equilibrium [10] is also used for client puzzle to defend against flooding attacks. Puzzle generation is the most important process in game theory as it should contain few uniqueness [15] in its future and they are the puzzle must be easier for the server to generate and it should be harder for the client to solve. And the puzzle computational cost must be lesser for the server than the client. Every client must be allotted only a short time to solve the puzzle.

The paper is organized as follows. Related works are discussed in Section 2. In Section 3 overview of the proposed methodology is given 5. Experimental setup, simulation parameter along with experimental results in Section 4. Finally, conclusion in Section 5.

2. RELATED WORKS

Some of the related works of the method proposed is given below

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Brent Waters et al., (2004) introduced a new technique to handle denial of service attacks. They use a robust external service called bastion for distribution. The author aims to provide unique puzzle solution, per-channel puzzle distribution, per-channel puzzle solution, random-beacon property, Identity-based key distribution and Forward security. The author declares that the method developed by them is more resistant in handling over 80% DoS over the existing methods. This method is cheap in applying at the IP level and at higher level of the protocol stock. The method also provides an opportunity to solve the puzzle in offline. Diffie – Hellman agreement is used for puzzle generation.

Mehran S. Fallah (2010) proposed a series of optimal puzzle-based strategies for handling increasingly sophisticated flooding attack scenarios. The author proposed four methods namely PDM1 for open-loop solution and which is not applicable when the payoff is higher, PDM2 proposed for closed loop solution but which is not capable in handling the single-source attacks, PDM3 for known coalition size is an extension of PDM2 which deals with distributed attacks and PDM4 in which the size of the attack coalition is assumed unknown.

Lakshmi Kuppusamy et al., (2012) proposed a number theoretic puzzle against denial of service attacks. They introduced a new variant of the interval discrete logarithm assumption problem and showed the hardness of this new problem under the factorization and composite interval discrete logarithm assumptions. The author declares that the puzzle proposed is much faster to verify than the existing number theoretic puzzles. for the 512-bit RSA modulus, the solution verification time of proposed is approximately 89 times faster when compared with Rivest et al. puzzle and by approximately 50 times faster when compared with Karame- Capkun puzzle.

T. Shanmugapriya et al., (2013) in their research work the optimal puzzle-based defense strategies are developed. The proposed method provides a complete flooding attack solution is likely to require some kind of defense during the attack traffic identification.

Vancha Maheshwar Reddy et al., (2013) suggest a Game theory based strategy to create a series of defense mechanisms using puzzles to defend against flooding attacks. Author used the concept of Nash equilibrium is used to handle sophisticated flooding attack to defend distributed attacks from unknown number of sources.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

3. OVERVIEW OF THE PROPOSED METHODOLOGY

The proposed method consists of few steps and they are discussed in detail in this section. The flow of the proposed method is given in figure.1

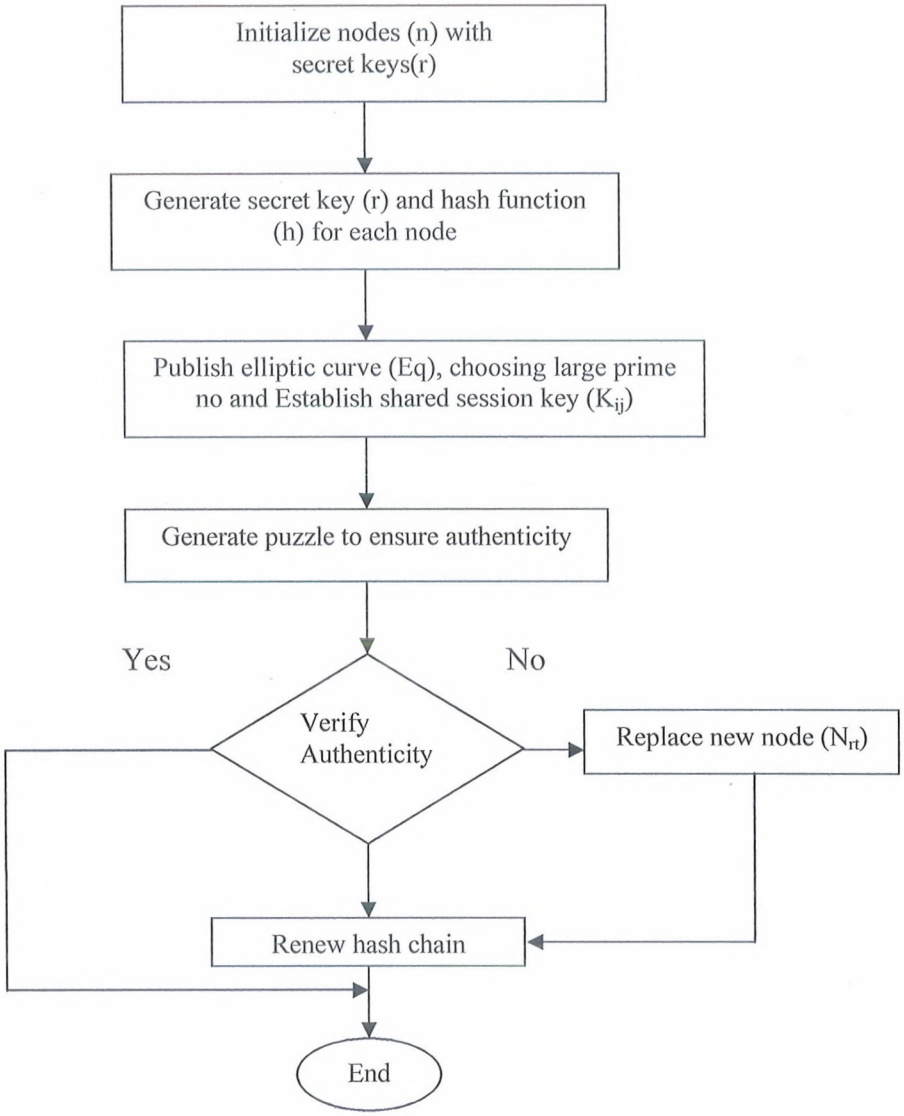

Figure.1 Flow of the proposed method

3.1. Steps of the Proposed Method

The proposed method consists of some phases which are discussed below in various sections. The notations used in the proposed method are given in following table:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Step.1 Initialization Phase

Initiates secret keys and hash function for the nodes of a designated are

Step.2 Authentication

Each node solves puzzle for authentication and key establishment between nodes.

Client puzzle is the process of sending the puzzle by the server to client before executing the client request. Upon receiving the puzzle, every client has to solve the puzzle within the given period of time in order to access the server. The puzzle generated by the server must be harder for the client to solve. The steps involved in client process are

Step 1 $C \rightarrow S$*: sending service request*
Step 2 S: generation of a puzzle
Step 3 $S \rightarrow C$*: sending a description of the puzzle*
Step 4 C: solving the puzzle
Step 5 $C \rightarrow S$*: sending solution to the puzzle*
Step 6 S: verification of the solution. If the solution is correct:
Step 7 S: continue processing a service request

Step.3Key establishment phase

Generate session key randomly to verify the authenticity of the node.

Step.4Elliptic Curve Cryptography on new node failure phase

Add new node on failure of any existing node with secret key, random number and ECC parameter.

Elliptic Curve Cryptography (ECC) is popular nowadays for key generation. The key will be generated using ECC is a shorter one. The benefits of using ECC help in reducing the energy consumption, lower bandwidth usage and execution will be faster when compared with other algorithms. ECC can be defined as

$$E: y^2+xy=x^3+ax^2+b$$

a,b ---> finite binary fields

x,y ----> set of all points on E

Step.5 Game theory on hash chain renewal phase

Renew the hash chain for the new node updated.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

3.2. Proposed Method Algorithm

Game theory plays a major role in security in recent years. In this phase the cyber attack is handled using game theory approach. The proposed method consists of few steps and they are discussed in detail in the following sections:

Table.1 Proposed Method Algorithm

```
Input:

S → Source Node
D → Destination Node

Procedure:
repeat
        for each neighbor nodes
       S sends a RREQ to all nodes
        check sequence number
         check key
          sends puzzle
do if nodes solves puzzle
          establish connection
         forward packets
       then stop
     end if
else
  exit
end
until end of the node
```

4. RESULTS AND DISCUSSIONS

The simulated environment, simulation parameter, performance metrics and results are discussed in detail in this section.

4.1 Simulation environment

The proposed methodology is simulated under Linux Fedora, using the Network Simulator NS2 version ns-allinone-2.35.

4.2 Simulation Parameter

The below table shows the simulation parameters used in this method:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Table.1. Simulation Parameter

Parameter	Value
Simulator	NS-2
Channel Type	Wireless
Number of nodes	20,40,60,80,100
Traffic Model	CBR
Maximum mobility	60 m/s
Terrain area	1000m x 1000m
Transmission Range	250m
Routing Protocol	AODV
MAC protocol	802.11
Observation Parameter	End to end delay, Packet loss, Throughput, Latency, Routing Overhead

4.3 Performance Metrics

The proposed methodology is evaluated for its efficiency using the following parameters.

Throughput

The network throughput is the average rate of successful message delivery over a communication channel. The throughput is usually measured in data packets per second or data packets per time slot i.e. number of bytes of data that is transferred per second between source and destination.

Routing Overhead

The total number of routing packets generated and forwarded at the time simulation

Average Packet Delivery Ratio

Average Packet Delivery Ratio is calculated for every 10 seconds. This performance metrics shows the efficiently the packets are delivered between the source and the destination. The packet delivery ratio is calculated using the following equation:

$$\text{Packet delivery ratio} = \frac{received packets}{sent packets} * 100$$

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Average End to End Delay

The performance of the proposed method is evaluated in terms of end-to-end delay. Total time utilized to transmit the data from source to the destination.

False Acceptance Rate

The false acceptance rate is a fraction of negative entry or unauthorised user was incorrectly identified as positive entry or unauthorised user and it will be calculated using the following formula:

$$\text{FAR} = \frac{number\ of\ false\ rejections}{number\ of\ client\ accesses}$$

False Rejection Rate

The false rejection rate is a fraction of positive entry or unauthorised user that was correctly identified as negative entry or unauthorized user and it will be calculated using the following formula:

$$\text{FRR} = \frac{number\ of\ false\ accep\tan ces}{number\ of\ client\ accessses}$$

4.4. Results

The results of the proposed method are presented in this section. The graphical representation of the results is also given below:

Table.2 Results of Throughput

Node	Existing Method	Proposed Method
20	1432	3987
40	3438	8908
60	7898	14343
80	14879	17809
100	21233	24569

Table.3 Results of Overhead

Node	Existing Method	Proposed Method
20	70	67
40	102	97
60	146	123
80	189	154
100	213	193

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Table.4 Results of Packet Delivery Ratio in Percentage

Node	Existing Method	Proposed Method
20	14	17
40	33	39
60	48	45
80	68	78
100	92	98

Table.5 Results of Delay

Node	Existing Method	Proposed Method
20	0.4522	0.3452
40	0.8431	0.6431
60	0.9272	0.8272
80	1.213	0.7563
100	1.33	1.1243

Table.6 Results of Packet Drop

Node	Existing Method	Proposed Method
10	14	12
20	35	26
30	46	38
40	52	43
50	65	56
60	77	63
70	82	78
80	92	86
90	121	108
100	156	138

Table.7 Results of Average No of claims (Based on time)

Time (Seconds)	True Positive	True Negative	False Positive	False Negative
10	2.3	4.0	6.5	9.0
20	2.4	4.2	6.3	8.9
30	2.5	4.3	6.3	8.9
40	2.5	4.4	6.1	8.7
50	2.6	4.5	6.0	8.6
60	2.9	4.6	5.9	8.6
70	3.0	4.6	5.8	8.6
80	3.2	4.7	5.6	8.5
90	3.7	4.9	5.5	8.5
100	4.1	5.2	5.4	8.4

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The average number of claims of the attacker and the defender is calculated and the results are given in the table. 7.

Cyber Attacks	Enhanced Game Theoretic Approach	Existing Method	% of Improvement
Active Attacks	**75%**	78%	**3%**
Passive Attacks	**69%**	71%	**2%**

The above table.8 shows the accuracy of the proposed method in detecting the cyber attacks.

5. CONCLUSION

In this research work secure hash based game theory approach is introduced to detect the unknown cyber attacks. Hash based client puzzle protocol is used along with elliptic curve cryptography. Every data or information communicated in this method is encrypted. The efficiency in detecting the unknown cyber attacks of the proposed method is evaluated in a simulated environment using network simulator NS2 ns2allinone 2.35. The proposed method detects the unknown cyber attacks and it also evaluated using performance metrics namely Throughput, Routing Overhead, Packet Delivery Ratio, End to end delay, Packet drop ratio, Average No of claims (Based on time and distance). Based on the evaluation result, the proposed method outperforms the existing method.

REFERENCES

[1]. Abhay Kumar Rai et al., "Different Types of Attacks on Integrated MANET-Internet Communication" International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), pp.265 – 274.

[2]. Priyanka Goyal et al., "A Literature Review of Security Attack in Mobile Ad-hoc Networks" *International Journal of Computer Applications (0975 – 8887)* Volume 9– No.12, November 2010, pp.11-15.

[3]. Dr. G. Padmavathi and Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" *International Journal of Computer Science and Information Security,. 4, No. 1 & 2, 2009,* pp.1-9.

[4]. Brent Waters et al., "New Client Puzzle Outsourcing Techniques for DoS Resistance" *CCS'04,* ACM, pp. 246-256.

[5]. Mehran S. Fallah, "A Puzzle-Based Defense Strategy Against Flooding Attacks Using Game Theory" IEEE Transactions on dependable and secure computing,Vol.7,No.1, p.5-19.

[6]. Lakshmi Kuppusamy et al., "Practical Client Puzzles in the Standard Model" ASIACCS '12, ACM.

[7]. Raju Neyyan, "Game Theory based Defense Mechanism against Flooding Attack using Puzzle" Emerging Trends in Computer Science and Information Technology - 2012(ETCSIT2012), pp.5-10.

[8]. T. Shanmugapriya et al., "Computational puzzles for repudiation of misbehaving users in anonymzing network", International Journal of Advances in Engineering & Technology, May 2013, Vol. 6, Issue 2, pp. 1032-1036.

[9]. Douglas Stebila et al., "Stronger difficulty notions for client puzzles and denial-of-service-resistant protocols" CT-RSA 2011, The Cryptographers' Track at the RSA Conference, LNCS, Springer, 2011volume 6558, pp. 284- 301.

[10]. Vancha Maheshwar Reddy, "Game Theory based Defense Strategy against Denial of Service Attack using Puzzles" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 1, January -February 2013, pp.751-757.

[11]. Animesh Patcha and Jung-Min Park, "A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks" International Journal of Network Security, Vol.2, No.2, Mar. 2006, PP.131–137.

[12]. Tansu Alpcan and Tamer Basar, "A Game Theoretic Analysis of Intrusion Detection in Access Control Systems" 43rd IEEE Conference on Decision and Control, 2004, pp.1568 – 1573.

[13]. Martin Rehak et al., "Game Theoretical Adaptation Model for Intrusion Detection System" Proc. of 10th Int. Conf. on Autonomous Agents and Multiagent Systems – Innovative Applications Track (AAMAS 2011), 2011, pp. 1123-1124.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[14]. Xiannuan Liang and Yang Xiao, "Game Theory for Network Security" IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, 2013, pp.472 – 486.

[15]. J.Jaikumar, "A Defense Strategy Against Flooding Attack using Puzzles By Game Theory" *International Journal of Computer Trends and Technology (IJCTT) - volume4Issue4 –April 2013*

[16]. Ari Juels and John Brainard, "Client puzzles: A cryptographic countermeasure against connection depletion attacks" P*roceedings of NDSS '99 (Networks and Distributed Security Systems)*. pp. 151–165.

BIOGRAPHIES

M.Uma is a Ph.D. research scholar of Avinashilingam Deemed University, currently doing research on cyber security. Her areas of interest include Information and communication Security. She has 5 publications in her research work. She is currently the principal investigator for one project funded by DST (WOS-A). She is a reviewer for WSEAS, IJSET and TIJCSA.

Dr.G.Padmavathi is the Professor and Head of computer science of Avinashilingam Deemed University for women, Coimbatore. She has 23 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication, Network Security and Cryptography. She has 100 publications in her reascher area .In presently she is guiding M.phil researcher and PhD's Scholar .She has been profiled in various Organizations her academic contributions. She is currently the principal investigator of four projects funded by UGC and DRDO.She is life member of many preferred organizations of CSI, ISTE, WSEAS, AACE, and ACRS.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500