ENHANCED MOVING TARGET DEFENSE MECHANISMS TO HANDLE CYBER ATTACKS

CHAPTER 5

Smart Motion Adaptation/Management using Game Theory

Handling unknown cyber attacks are more challenging than handling known cyber attacks. The game changing approach is one of the significant cyber attack handling mechanisms. The three prominent game changing methods are tailored trustworthy spaces, moving target defense and cyber economics. There are 11 moving target defense mechanisms available in the literature [98]. Out of which four significant moving target defense mechanisms are considered in this thesis for enhancement. They are

i. **Smart Motion Adaptation/Management – Game Theory**
ii. **Robust Cryptographic Authentication – Mouse Dynamics**
iii. **Data Chunking and Decentralization**
iv. **Decoys**

Smart Motion Adaptation/Management - Game Theory approach is discussed in this chapter and enhanced using ECC(Elliptic Curve Cryptography) and puzzle solving for authentication.

The first moving target defense mechanisms taken in this research work are Smart Motion Adaptation/Management using a game theory approach[7][35][36][54][58] to defend against cyber attacks[66][92] and to ensure neighbor authentication.

5.1. Proposed Method using Enhanced Game Theory

The main aim of this proposed method is detection of cyber attacks and ensuring the neighbor authentication.

5.2. Phases of the Proposed Research Work

The proposed method consists of some phases which are discussed below in various sections.

5.2.1.Flow diagram of the Proposed Method

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.5.1

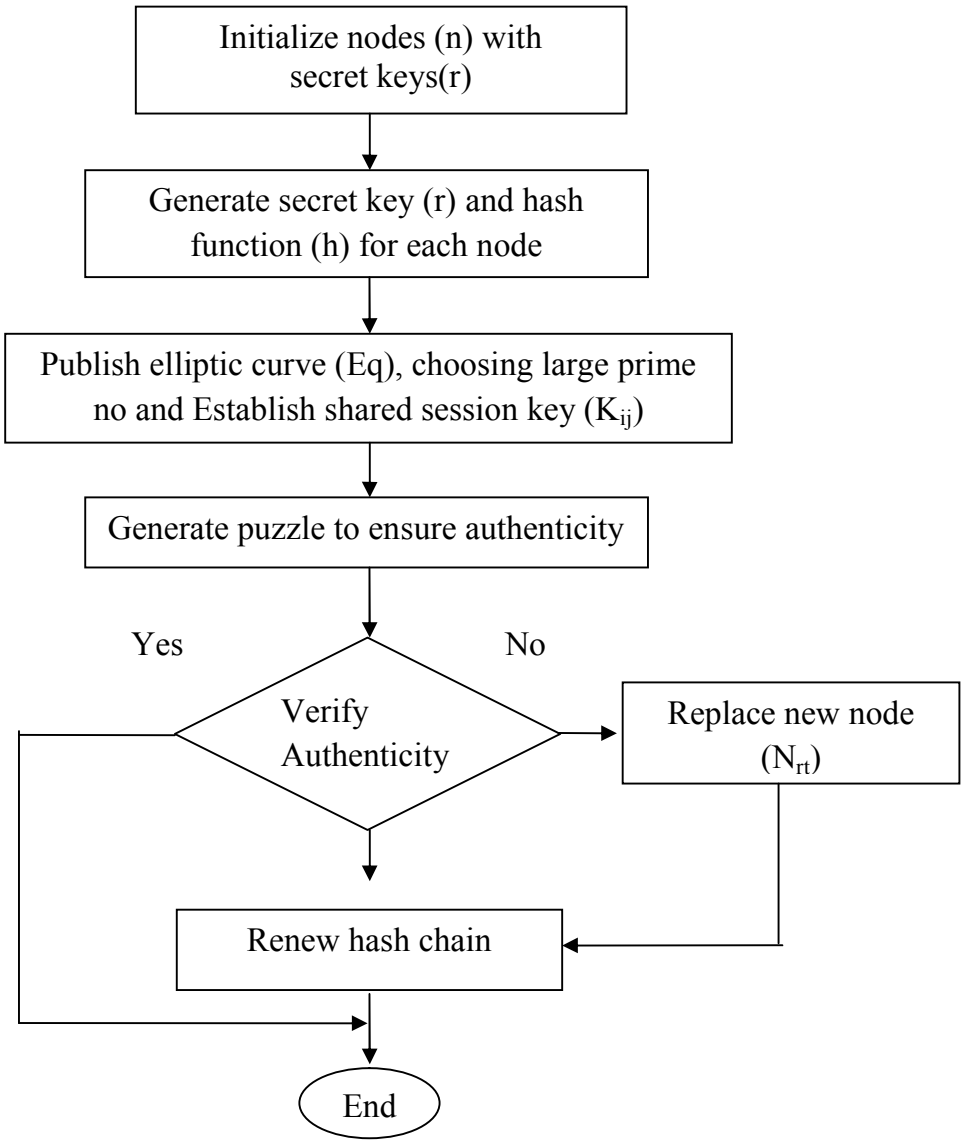

Figure.5.1 Flow diagram of the Proposed Method

Key Establishment Phase

Step.1

The RouteRequest (RREQ) will be initialized to the neighbor node when there is a data packet that is to be sent from source to the destination.

Step.2

After receiving the RouteReply (RREP) from the neighbor node, secret session key will be generated and verified with the neighbor to check whether the node is a legitimate node. This process will be executed for each neighbor node till destination node.

Step.3

In case of any node failure, the new node will be injected or updated in the hash chain and verified for authentication.

Step.4

After key verification, renewal of hash chain will be updated upon request.

5.2.2. Steps Involved in this Research Work

The enhanced game theory method steps are discussed below.

Step.1 Initialization Phase

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

Step.2 Authentication

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

Client puzzle[13][46][56][79][82][86] 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 $C \rightarrow S$: *send the service request*
Step 2 *S: generate a puzzle*
Step 3 $S \rightarrow C$: *send a description of the puzzle*
Step 4 *C: solve the puzzle*
Step 5 $C \rightarrow S$: *send the solution to the puzzle*
Step 6 *S: verify the solution: If the solution is correct then go to step 7 else go to step 8*
Step 7 *S: continue the process for next service request*
Step 8 *Stop*

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 a 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

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

F_2*- finite binary fields*

a,b *– constant* ϵF_2

x,y *– is a points on Elliptic curve E*

Step.5 Game theory on hash chain renewal phase

Renew the hash chain for the new node updated.

5.2.3. Proposed 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.5.2 Proposed Algorithm

```
Input:
S → Source Node
D → Destination Node
Procedure:
repeat
        for each neighbor nodes
        S sends a RREQ to all nodes
        check sequence number
        checks key
       sends puzzle
   if nodes solves puzzle
          forward packets
      else
          packet not sent
   end if
until end of the node
```

5.3. Performance Metrics

The proposed methodology is evaluated for its efficiency using the following parameters and they are clearly defined in the previous chapters.

Throughput

Routing Overhead

Average Packet Delivery Ratio

Average End to End Delay

False Acceptance Rate

False Rejection Rate

5.4. Simulation Environment

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

5.4.1. Simulation Parameter

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

Table.5.3. Simulation Parameter

S.No	Parameter	Value
1	Simulator	NS-2
2	Channel Type	Wireless
3	Number of nodes	20,40,60,80,100
4	Traffic Model	CBR
5	Maximum mobility	60 m/s
6	Terrain area	1000m x 1000m
7	Transmission Range	250m
8	Routing Protocol	AODV
9	MAC protocol	802.11
10	Observation Parameter	End to end delay, Packet loss, Throughput, Latency, Routing Overhead

5.5. Results and Discussions

The results of the proposed method are presented in this section. The graphical representation of the results is also given below. The attack packets are also injected along with the normal data packets. Four attacks were injected for 20 nodes, likewise 8, 12,16, 20 for 40,60,80 and 100 nodes. The results show the efficiency of the proposed method before and after injecting the attacks.

Table.5.4. Results of Throughput

Time (Sec)	Existing method before Attack Injection	Proposed method after after attack Injection
20	1432	3987
40	3438	8908
60	7898	14343
80	14879	17809
100	21233	24569

Table.5.4 shows the results of the throughput before and after the attacks. It shows the successful delivery of data packets for every 20 seconds.

Table.5.5. Results of Overhead

Time (Sec)	Existing method before Attack Injection	Proposed method after after attack Injection
20	70	67
40	102	97
60	146	123
80	189	154
100	213	193

In Table.5.5, the result of routing overhead is shown. The efficiency of the proposed methods is increased even after the attack is increased.

Table.5.6. Results of Packet Delivery Ratio

Time (Sec)	Existing method before Attack Injection	Proposed method after after attack Injection
20	14	17
40	33	39
60	48	45
80	68	78
100	92	98

The packet delivery ratio is calculated for every 20 seconds and the efficiency of the proposed method even under attack is clearly depicted in Table.5.6.

Table.5.7. Results of End to End Delay

Time (Sec)	**Existing method before Attack Injection**	**Proposed method after after attack Injection**
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

In Table.5.7 the results are obtained shows the performance efficiency of the proposed method for end to end delay. The average end to end delay is measured for every 20 seconds and improvement to the existing performs better under all circumstances.

Table.5.8. Results of Packet Drop

Time(sec) in %	Existing method before Attack Injection	Proposed method after after attack Injection
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

The packet drop ratio of the proposed method is calculated for every 10 seconds is depicted in Table.5.8, even under attack the drop ratio is minimized.

Table.5.9 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

The average number of claims of the attacker and the defender is calculated and the results are given in Table. 5.9.

Table.5.10 Cyber Attack Detection Rate

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

The above Table.5.10 show the accuracy of the proposed method in detecting the cyber attacks.

5.6. Chapter Summary

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. 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). Based on the evaluation result, the proposed method outperforms the existing method. The percentage of detection rate is increased to 3%. The proposed method detects 71% of cyber attacks. For better performance the next moving target mechanism robust cryptographic authentication using mouse dynamics is implemented and discussed in the next chapter.