ENHANCED MOVING TARGET DEFENSE MECHANISMS TO HANDLE CYBER ATTACKS

CHAPTER 8

DECOYS AND EVALUATION OF THE PROPOSED METHODS

This phase is classified into two sections. First section discusses about the fourth moving target defense mechanisms taken for this research work. In the second second, the evaluation of the four moving target defense mechanisms is compared in terms of attack detection rate.

Security is an important challenges in the cyber world. Security goals such as confidentiality, availability, integrity, non-repudiation, authentication and authorization should be ensured in every communication process. Though, available methods in the literature handle the security threats effectively, other new challenges come in terms of more smart and unknown attacks. Many cyber attack handling mechanisms are discussed in the literature. The four moving target defense mechanisms are

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

Decoys involve the process of providing a number of fake targets, so that the authorized users can be easily identified from the attackers. Due to these fake targets the attackers will be diverted from the real target, whereas the progression by the attacker will get down slowly, by this time the attacker will be confounded. During this time, the authorized user will access the data or information without any interruptions.
Time triggered and event triggered approaches are integrated to increase the attack detection rate.

8.1. Proposed Integrated Time and Event Triggered Approach

The time-triggered [70][91] and event-triggered [80] [89] approach play a noteworthy role in securing the data or information. AntNet protocol [55][67] is also used in the proposed approach. In this method, one to five nodes are placed as fake

targets to monitor the network. The processing of time triggered approach [42] [51] will function in a synchronized way. The advantages of this approach are:

- The communication in this approach will be executed in a systematic manner.
- This approach does not require any addressing scheme as the dispatching table will look after the packets communicated at a specific point of time.
- Time triggered approach helps every node to be aware of the processing node at present.

As the time triggered uses the predefined timing, it enables to gather the entire details of packets like sending time and receiving time which help to measure the potential of the protocol used. Though it performs well in communication, it has certain limitations given below.

Specific lacking features with the time triggered are as follows:

- If any interrupt occurs during sending or receiving packets, the time triggered approach will not communicate to the controller.
- The bandwidth will be equally allotted for every node in a network. Sometime if any node needs more bandwidth, the time triggered approach is not capable of allocating the same dynamically.
- Adding or removing a node in network without modifying the structure of the network is not possible in time triggered approach.

To enhance its efficiency, it is necessary to overcome the above said limitations. So research work aims to integrate time triggered approach with the event triggered approach.

8.1.1. Phases of this Research work

The aim of this research work is to prevent data or information communicated in the network from cyber attacks and to provide Quality of Service.

The primary focus of this research work is to provide security while transmitting the data from the source node to the destination.

In the simulated network, the source node broadcasts about the data packets (RREQ). The nodes will be selected as a group based on the route reply (RRER). The

selected nodes will be checked with the sequence number and then the data packets will be forwarded. The packets will be forwarded at the given point of time. The time schedule of the time triggered approach is given in figure. 8.1.

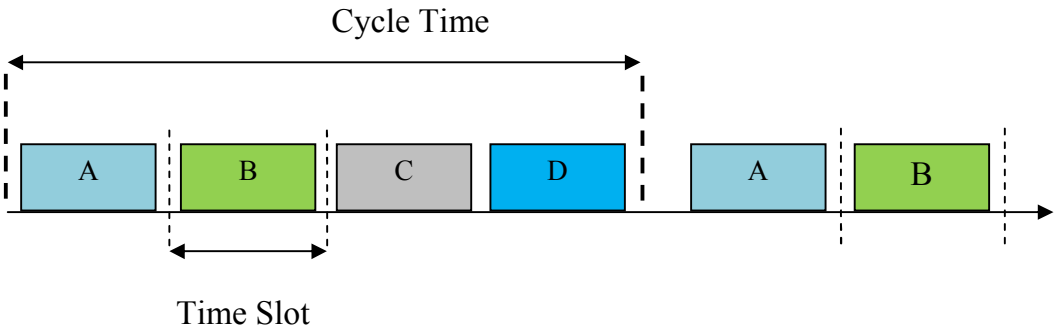

Figure.8.1. Time Triggered Approach

The above diagram clearly depicts about the execution of the time triggered approach [87]. For every communication, a predefined time will be allotted for each node. Before communication the node authentication is verified by sequence number and a secret key. The time schedule for every node will be given in a table; the data communication will be executed according to that. All the communication is encrypted and decrypted. In case of any events the event triggered will be initiated. Event triggered acquire more flexibility and adaptability. The execution of event triggered approach is given in figure. 8.2.

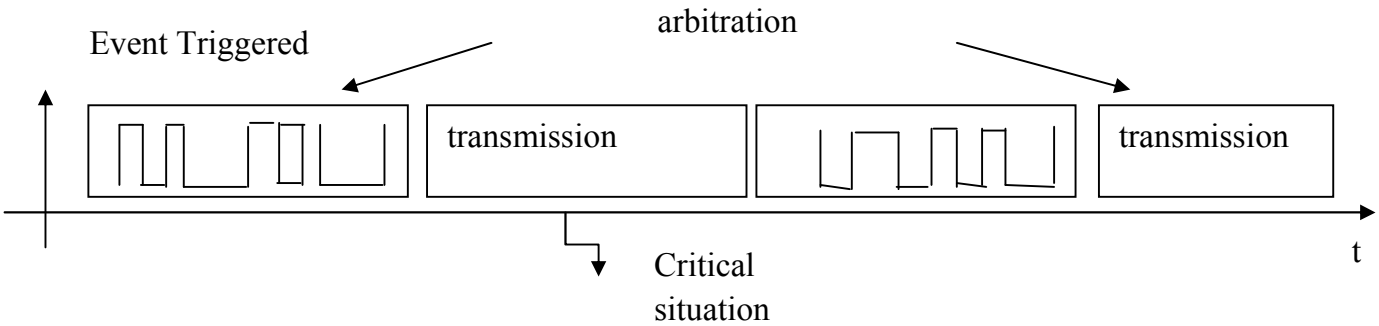

Figure.8.2.Execution of Event Triggered Approach

The above diagram clearly states the execution of the event triggered approach. Both time triggered and event triggered are integrated and a new approach is developed. The header format of the proposed method is given in Table. 8.1.

Table.8.1. RREQ control message format of the proposed method

Type 1	J	R	D	G	Reserved	Hop count
RREQ ID						
State Transition	Encryption	DeamonActions	Decryption			
RREQ time	RREQRecv strength	RREQ info				
Destination IP Address						
Destination sequence Number						
Originator IP Address						
Originator sequence Number						
Path Node IP Address						
Path Node Sequence Number						

Type 1

J-Join flag,

R-Repair flag,

G-Gratuitous RREP flag; indicates about a gratuitous RREP to the node specified in the Destination IP Address field.

D-Destination flag; indicates only the destination may respond to this RREQ, Reserved: Sent as 0; ignored on reception,

Hop Count: The number of hops from the Originator IP Address to the node handling the request.

RREQ ID: A sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address.

State Transition: In the state transition the ant selects the node which has more pheromone. Thus the probability will be measured using the following equation

$$P_{ij}^{d} = \{ (\tau_{ij}^{k} / \sum_{j \subset N_i} \tau_{ij}^{k}) \; if \; j \in N_i \}$$

where,

α *and* β means heuristic information and importance of the pheromone which can affect the choice of the ants.

$\tau_{ij}\ (t)$ Means the pheromone trail;

$\eta_{ij}\ (t)$ Means a locally available heuristic information, generally, $\eta_{ij}\ (t) = 1/d_{ij}\ (t)$

J_k (i) Means the nodes gather ant has not visited.

Daemon Actions: Once solutions have been constructed, and before updating the pheromone values, often some specific actions may be required and that are *daemon actions*, and can be used to implement problem specific and/or centralized actions, which cannot be performed by single ant. The most used daemon action consists in the application of local search to the constructed solutions: the locally optimized solutions are then used to decide which pheromone values to update.

Destination IP Address: **T**he IP address of the destination for which a route is desired.

Destination Sequence Number: The latest sequence number received in the past by the originator for any route towards the destination.

Originator IP Address: The IP address of the node which originated the Route Request.

Originator Sequence Number: The current sequence number to be used in the route entry pointing towards the originator of the route request.

8.1.1.1. Flow diagram of the Proposed Method

The few steps of the integrated time triggered and event triggered approach are given in figure. 8.3

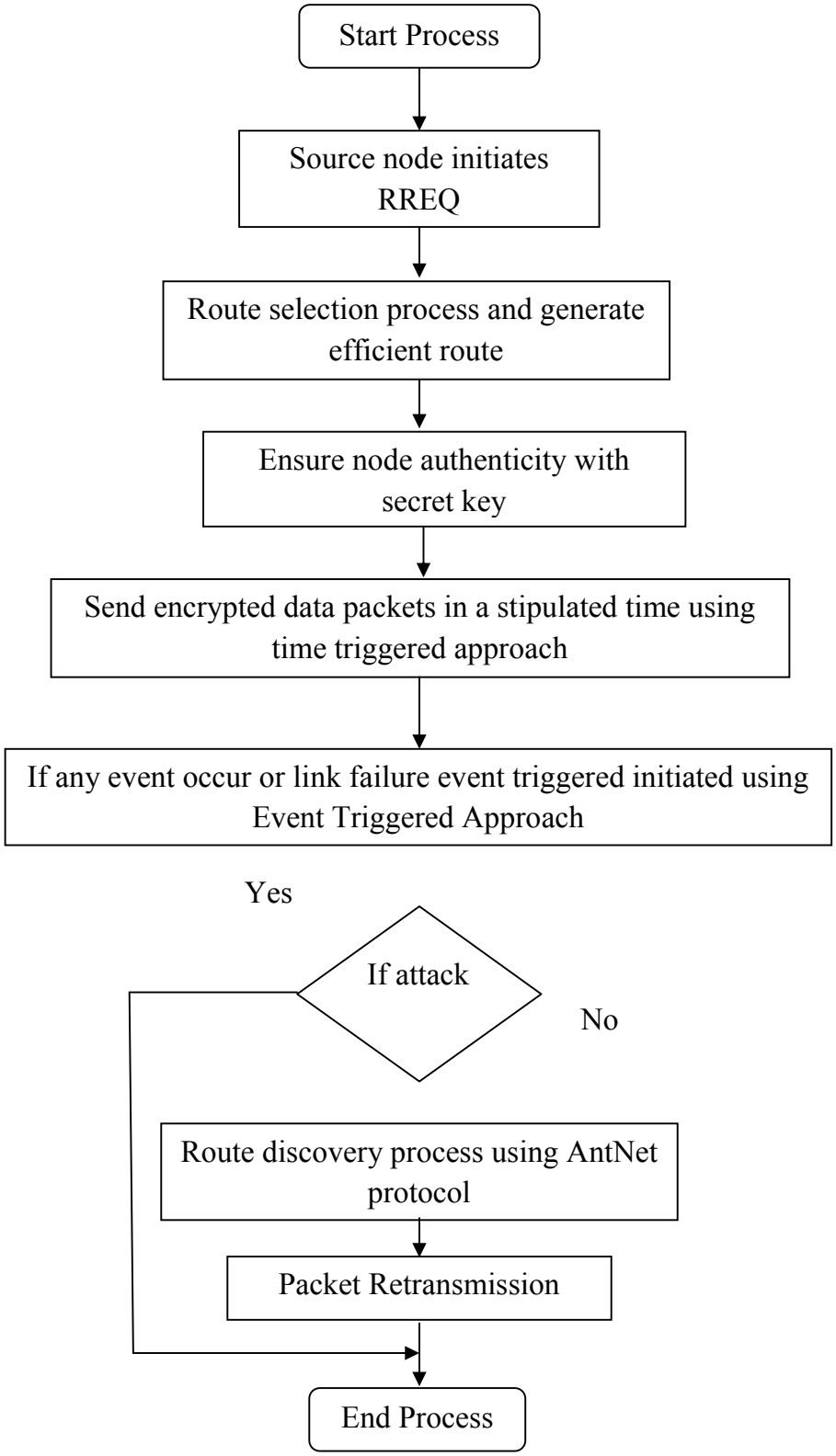

Figure.8.3 Flow of the proposed method

8.1.1.2.Steps of the Integrated Method

The algorithmic steps of the new integrated approach are as follows:

Step.1 *The source node broadcast about the data packet and initiates RREQ*

Step.2 *Route Selection Process (RRER)*

Step.3 *Ensure node authenticity with secret key*

Step.4 *Time Triggered approach sends the encrypted packets to all the nodes with in a pre-defined time.*

Step.5 *If any event occurs or any node doesn't receive data packets will be communicated to the controller by event triggered approach initiated.*

Step.6 *AntNet Protocol for route discovery process*

Step.7 *Event triggered retransmits data packets to node which doesn't receive the data.*

8.1.1.3. Proposed Algorithm

The algorithmic steps of this research work is given in Table.8.2

Table.8.2 Proposed Algorithm

```
S → Source Node
D → Destination Node
Repeat
  for each neighbor nodes in the network
    S sends a RREQ to all nodes
      S receives the RRER from other nodes
          check sequence number
   if route exists then
     forward packets
     if TTL (Time to live ) is exceeded then
       stop
     else
       neighbor node does not receive any packets within a given
         time
       event triggered protocol receives message from node
      assigns AntNet for route discovery and route maintenance
     end if
  end if
 end`
until route is expired
```

To evaluate the proposed method some of the performance metrics are used and they are discussed below in detail.

8.1.2. Performance Metrics

The objective of the simulation is to enhance the security and Quality of Service with this new approach of Time Triggered and Event Triggered. The performance of the integration of Time and Event Triggered approach is evaluated in terms of performance metrics like

Average Packet Delivery Ratio,

Average Throughput

Average End-to-End Delay

Average Latency

Average Routing Overhead

Energy Consumption

Average Packet Delivery Ratio

Average Packet Delivery Ratio is calculated for different number of nodes like 20,40,60,80 and 100 for an area of 1000m x 1000m. This performance metrics shows how efficiently the packets are delivered from the source to the destination. The packet delivery ratio is calculated using the following formula:

$$\text{Packet delivery ratio} = \frac{received\ packets\ at\ destination}{sent\ packets\ at\ source}$$

Average Latency

The time taken to send a unit of data between two points in a network is termed as latency.

Average Routing Overhead

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

Energy Consumption

The total units of time required for transmitting the key among the nodes during the simulation time are known as energy consumption.

8.1.3. Simulation Environment

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

8.1.3.1. Simulation Parameters

The below Table.8.3 shows the simulation parameters used in this method:

Table.8.3. Simulation Parameters

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,FSR,OSPF, RIP, AntNet
MAC protocol	802.11
Observation Parameter	End to end delay, Packet loss, Throughput, Latency, Routing Overhead and Energy Consumption

8.1.4. Results and Discussions

The main goal of this research work is to detect the unknown cyber attacks without compromising Quality of Service; the following section gives the results of the performance metrics used to evaluate the proposed method in comparison with other methods.

Table.8.4 Comparative results of the proposed method

Performance Metrics	Time Triggered Approach					Event Triggered Approach					Integrated Time and Event Triggered Approach					Integrated Time and Event Triggered Approach with AntNet Protocol				
	Time(Seconds)																			
	2	4	6	8	10	2	4	6	8	10	2	4	6	8	10	2	4	6	8	10
End to End Delay	0.82	0.90	0.93	0.94	0.95	0.94	0.94	0.95	0.96	0.96	0.34	0.82	1.24	1.33	1.43	**0.18**	**0.31**	**0.23**	**0.45**	**0.49**
Packet Delivery Ratio(in Percentage)	90.4	91.7	93	92.3	94	87	89	90	91.2	93	80	80.8	82	84	85	**94.7**	**95**	**96**	**96.7**	**96**
Routing Overhead	5200	6900	8300	9800	11000	9000	11000	12000	13670	14720	4000	4440	4490	4920	5250	**3000**	**3100**	**3200**	**3200**	**3400**
Latency	1.0	1.06	1.05	2.09	2.15	1.82	1.9	1.92	1.08	1.55	0.93	0.97	1.0	1.1	1.07	**0.6**	**0.68**	**0.73**	**0.80**	**0.84**
Throughput	3400	3450	3570	3710	3750	2800	2860	2920	3000	3360	3000	3170	3230	3270	3300	**4000**	**4280**	**4330**	**4410**	**4780**
Energy Consumption	942	950.2	958.4	963	967	953	955	961	978	993	849	911	933.1	924	950	**924**	**932**	**945**	**972**	**988**

Table.8.5 Cyber Attack Detection Rate

Attack Types	Integrated Time and Event Triggered Approach	Integrated Time and Event Triggered Approach with AntNet	% of Improvement
Active Attack	68%	71%	3%
Passive Attack	78.5%	83%	4.5%

Table.8.4 and Table.8.5 clearly show the efficiency of the proposed method. The method proposed helps to increase the packet delivery ratio and throughput and reduces the end to end delay, routing overheads and latency. However, the energy consumption is more in the proposed method which has to be reduced in future work.

8.2. Evaluation of the Proposed Methods

In recent years, cyber attacks have become a major challenge to the entire communication world. Due to known and unknown cyber attacks every country is facing huge economic loss. Though many handling mechanisms are available, some more efficient mechanisms are still needed. Recently, game changing approaches have been found to be an appropriate solution to handle cyber attacks.

The goal of this research work is to improve the efficiency of the existing methods to handle the cyber attacks and providing the Quality of Service in a networking environment. In this research work, the existing methods are well analyzed. According to the literature survey four moving target defense mechanisms are enhanced. An additional feature is added to the existing network traffic monitoring method. Principal Component Analysis, a linear dimensionality reduction technique is enhanced with optimization technique to increase the accuracy in detecting the known cyber attacks.

The proposed methods achieve a higher level of accuracy in detecting unknown attacks. The comparative results are given in Table. 8.6. Integrated Time and Event triggered approach outperforms the other three methods.

Table.8.6 Evaluation Results of the Four Proposed Methods

S.No	Methods	Attack Detection Rate
1	Improved Game Theory Approach	71%
2	Enhanced Click Dynamics	**73%**
3	Data Chunking and Decentralization	79%
4	Time and Event Triggered Integrated Approach	**83%**

8.3. Chapter Summary

Security is very essential for communication in both wired and wireless networks. The various cyber attacks and defense mechanisms to handle cyber attacks are analyzed in this research work. As suggested by the expert committee of the National cyber leap year summit, decoys is taken to develop a mechanism to defend against unknown cyber attacks. In this research work, the time triggered and event triggered approaches are analyzed. A new approach is developed by integrating the two methods along with the computational intelligence technique AntNet protocol. The performance of the proposed approach is analyzed in terms of Throughput, End to End delay, Routing Overhead, Packet Delivery Ratio, Latency and Energy Consumption. The results show that the proposed approach makes better possibility of detecting and defending against cyber attacks.

The four moving target defense mechanisms are taken for this research work. For each method the improvement and enhancement are proposed. Based on the cyber attack detection rate, the improved moving target defense mechanisms are compared.