International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 9, Number 22 (2014) pp. 12977-12989

http://www.ripublication.com

Enhanced Decoy based Moving Target Defense Mechanism with Improved Quality of Service to Handle Cyber Attacks in Wireless Networks

M. Uma[1] and Dr. G. Padmavathi[2]

Ph.D Research Scholar[1], Department of Computer Science
Avinashilingam Institute for Home Science and Higher Education for Women
Coimbatore-641043, Tamilnadu, India.
uma.phdresearch@gmail.com[1]
Professor and Head[2], Department of Computer Science
Avinashilingam Institute for Home Science and Higher Education for Women
Coimbatore-641043, Tamilnadu, India
ganapathi.padmavathi@gmail.com[2]

Abstract

Cyber attacks are becoming a major challenge in today's connected environment. More personal devices are connected and operated in a wireless environment. Securing the wireless network needs better solutions in terms of its quality of service. There are many methods available in the literature to handle cyber attacks. Moving target defense mechanism is one of the upcoming and promising mechanisms to handle cyber attacks. Decoys, one of few moving target defense mechanism that is rarely explored. Time triggered approach and Event triggered approach are the two current approaches that dynamically help to secure the data in decoys defense type. The very important aspect to be noted here is that most of the methods provide security with compromised Quality of Service. To overcome this, while handling cyber attacks, an integrated time and event triggered method with AntNet protocol is proposed. The key feature of the proposed method is to defend the wireless networks against cyber attacks and to ensure Quality of Service (QoS) while handling the attacks. The effectiveness of this system is validated by conducting various experiments. The proposed method can identify the unauthorised user i.e. attacks in a precise way. The performance of the proposed method is evaluated based on the metrics like end to end delay, throughput, routing overheads, packet delivery ratio, latency and energy consumption. The proposed methodology is tested in a simulated environment with Linux Fedora and Network Simulator NS2 version ns-allinone-2.35.

Keywords: Decoys, Quality of Service (QoS), Cyber Attacks, Time triggered, Event triggered, AntNet Protocol

1. Introduction

Usage of Wireless technology in day to day activities is increasing day by day. Security issues are the challenging aspect for every advanced innovative research. Security goals such as confidentiality, availability, integrity, non-repudiation, authentication and authorization should be ensured in every communication process. Even, access by the authorized user is difficult today due to lot of cyber attacks and highly secured approaches are required for user authentication and verification. Due to increased number of cyber attacks, it is very crucial to protect our data, information from those attackers and from the hackers. Though there are number of promising techniques available for security, more advanced techniques are still upcoming and required for secured communication. Many cyber attack handling mechanisms are discussed in the literature [17][18][19][20]. Each technique is devised with some significant goals. However, new challenges are coming daily in terms of more smart and unknown attacks [14][15][16].

According to National Cyber Leap Year Summit 2009 Co-Chairs' Report, game changing approaches are the upcoming promising methods in handling cyber attacks. One among them is Decoys. The concept behind decoys is to place fake system to capture the attack and its pattern. It performs like a sensor node which predicts the attacks and the pattern of attacks. A decoy is one of the moving target defense mechanisms which can handle cyber attack in a compromised environment. The two approaches in decoys are namely, the time triggered approach and the event triggered approach. While handling the cyber attacks, the important point that is over looked or challenging especially in a wireless network is the Quality of Service. This research work aims at providing a decoy based moving target defense mechanism to handle cyber attacks with improved quality of service in a wireless environment.

The remainder of this paper is organized as follows: – the next section gives the details about the decoy based time triggered and event triggered approaches applied. Section 3 describes in detail about the proposed approach. Experimental results are presented in Section 4. Section 5 gives the conclusion of the research work.

2. Related works

The different types of cyber attacks and the various cyber attack handling mechanisms are available in the literature [17][18][19][20]. The different types of moving target defense mechanisms are Data Chunking and Decentralization, Decoys, Robust Cryptographic Authentication, Smart Motion Adaptation/ Management. Decoys, one of the moving target defense mechanisms use two approaches namely, the time triggered and the event triggered approaches. A brief literature study is done with reference to the applications of these two decoys based approaches.

Robert Leidenfrost and Wilfried Elmenreich (2009) The method described in this paper applies the Reach back Firefly Algorithm on battery powered low-cost

wireless nodes to establish a wireless time-triggered network with a global notion of time. These events must be globally coordinated by the use of rounds and are stored in a file called Round Description List (RODL) file. Unfortunately, the test bed system suffered from an unexpected delay jitter and an additional communication delay. For this reason, the test bed results consider highly multi-hop topologies and the simulation results showed low delay jitter.

Christopher Szilagyi and Philip Koopman (2009) introduced an approach for authentication in time-triggered applications which prevents both masquerade and replay attacks. In this research, consideration is given only to time-triggered applications. In a real-time system, all the communication and processing activities are initiated at predetermined points of time with priori designated clock tick. In this research work, a system is built upon an approach to authenticate time-triggered communications by validating truncated MACs across multiple packets. This approach enables per-message authentication of reactive control messages and delayed authentication of state changes at a slight increase in the probability of induced failures. This approach also enables a tradeoff among per-packet authentication cost, application level latency, tolerance to invalid MACs and probability of induced failures to provide flexibility for system designers.

Ahmed Helmy (2000), in their research work present a new methodology for developing systematic and automatic test generation algorithms for multipoint protocols. These algorithms attempt to synthesize network topologies and sequences of events that stress the protocol's correctness or performance. The authors have introduced the concept of transition classification and completion to distinguish between transient and stable states and identified two types of transitions; externally triggered (ET) and internally triggered (IT) transitions. The former is stimulated by events external to the system, whereas the latter is stimulated by events internal to the system. Two algorithms for test generation are done namely, the fault-independent test generation (FITG) and the fault-oriented test generation (FOTG). FOTG is a better fit for robustness studies since it targets faults directly. The complexity for FOTG was quite manageable for the case study. Corrections to errors captured in the study are proposed with the integrated PIM-DM specification.

Apart from security related issues, time and event triggered approaches are applied in routing also.

Frank Bohdanowicz (2010), developed a new distance vector algorithm to solve the problem of Routing loops using Metric-based Topology Investigation (RMTI) protocol based on event-triggered updates. The research work is done with computer network based on virtual linux machines connected by software bridges to compare the convergence time of routing protocols.

The efficiency of the method is evaluated for both online and offline mode of operations. The RMTI algorithm shows two important advantages: the possibility to avoid *counting to infinity* (CTI) situations and to converge much faster than other distance vector algorithms in case of a topology change. The ability of RMTI to choose whether to optimize fast topology change detection or a traffic reduction (or a mixture of both) makes the test environment adaptable to the specific needs of many different networks.

This section briefly discussed the different decoys approach in varied challenges in wires networks. The proposed methodology is presented in the coming section.

3. Proposed Method

Decoys involve the process of providing more 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. Because of this, the progression by the attacker will get down slowly, by this time the attacker will be confound. During this time, the authorized user will access the data or information without any interruptions.

Time triggered approach helps every node to be aware of the current 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. Though it performs well in communication, it has some limitations which are given below:

- If any interrupt occurs during sending or receiving packets, the time triggered approach will not communicate to the controller.
- The bandwidth will be equally alloted 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.

These shortcomings indirectly help the attackers in many ways. While integrating time triggered approach with event triggered, the above shortcomings can be eliminated. for better route discovery AntNet protocol is used.

3.1. Phases of this research work

The header format of the proposed method is given in table.1
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,

Table.1 RREQ control message format of the proposed method

Type	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						

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

$$P_{ij}^{\ k}(t) = \begin{cases} \dfrac{[\tau_{ij}(t)]^{\alpha} * [n_{ij}]^{\beta}}{\sum_{u \in J_k(t)} [\tau_{tu}(t)]^{\alpha} * [n_{tu}]^{\beta}} & if \quad j \in J_k(i) \quad Other \\ 0 \end{cases}$$

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:
The 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.

3.2. Flow of the proposed method

This proposed method aims to prevent data or information communicates in the network from cyber attacks and to provide Quality of Service. The steps of the proposed method are discussed in detail in figure.1 and in table.2

Table.2 Proposed Algorithm

```
S → Source Node
D→ Destination Node
Repeat
  for each neighbor nodes in network
    S sends a RREQ to all 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
```

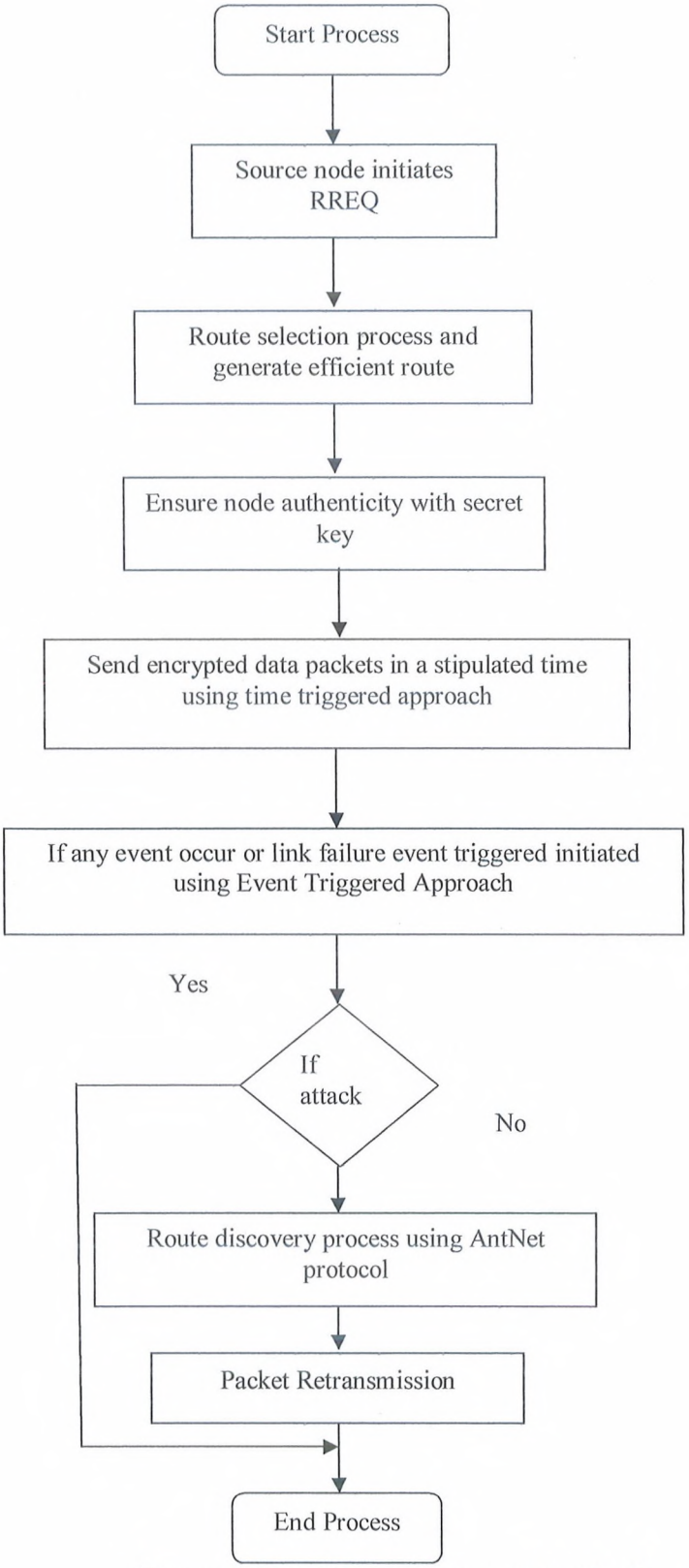

Figure.1 Flow of the proposed method

3.2. Steps of the proposed method

The proposed method algorithm is given in table.1. The steps involved are given below:

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.

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

4. Experimentation and Results

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

4.1 Performance Metrics

The performance metrics used in this method are given below. Along with the normal data packets, attacks are injected.

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 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.

$$Throuhput(\%) = \frac{\text{Re}ceivedpackets}{Sentpackets} * 100$$

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.

$$delay = \frac{1}{nbx} \sum_{i \in x} \sum_{iey} \frac{delay_j}{nby}$$

x: is the set of destination nodes that received data packets.
nbx: is the number of receiver nodes
y: is the set of packets received by node i as the final destination.

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 during the simulation time is known as energy consumption.

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

4.3. Simulation Parameters
The below table.3 shows the simulation parameters used in this method:

Table.3. 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,FSR,OSPF, RIP, AntNet
MAC protocol	802.11
Observation Parameter	End to end delay, Packet loss, Throughput, Latency, Routing Overhead and Energy Consumption

The result of the simulation is given in this section. The proposed method is evaluated by conducting the experiments. Table.4 and Table.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.

Table.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.5 Cyber Attack Detection Rate

Attack Types	Existing Method	Proposed Method	% of Improvement
Active Attack	68%	**71%**	**3%**
Passive Attack	78.5%	**83%**	**4.5%**

5. Conclusion

Security is very essential for communication in both wired and wireless networks. The various cyber attacks and defense mechanisms to handle cyber attacks are

analysed in this research work. As suggested by the expert committee of the National cyber leap year summit, decoys are taken to develop a mechanism to defend against unknown cyber attacks. In this research work, the time triggered and event triggered approaches are analysed. 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 proposed methodology is simulated under Linux Fedora, using the Network Simulator NS2 version ns-allinone-2.35.The results show that the proposed approach makes better possibility in detecting and defending against cyber attacks.

Acknowledgement
This work is supported by Department of Science and Technology, Government of India under Women Scientist Scheme (WOS-A).

References

[1]. Chris Szilagy and Philip Koopman, "Flexible Multicast Authentication for Time-Triggered Embedded Control Network Applications" *Proceedings of International conference on dependable systems and networks, DSN09*, pp.1-9.
[2]. Dan Pei et al., "An analysis of convergence delay in path vector routing protocols" *Computer Networks, Elsevier* 2005, pp.1-24.
[3]. Deepinder Sidhu, "*Open Shortest Path First (OSPF) Routing Protocol Simulation*", *SIGCOMM'93, ACM*, pp.53 – 62
[4]. Jaeok Park and Mihaela van der Schaar, "The Theory of Intervention Games for Resource Sharing in Wireless Communications" *IEEE Journal on Selected Areas in communications*, Vol. 30, No. 1, pp.165 – 175
[5]. John Rushby, "Systematic Formal Verification for Fault-Tolerant Time-Triggered Algorithms" *IEEE Transactions on software engineering*, Vol.25, No.5, 1999, pp.651 – 661
[6]. Liqi Shi and Abraham O. Fapojuwo, "TDMA Scheduling with optimized energy efficiency and minimum delay in clustered wireless sensor networks" *IEEE transactions on mobile computing*, Vol.9, No.7,2010, pp.927 – 940.
[7]. Liu Yingqiu, Li Wei, Li Yunchun, "Network Traffic Classification Using K-means Clustering" *IEEE Second International Multi-symposium on Computer and Computational Sciences*, 2007 pp.360 – 365.
[8]. Marcio Juliato and Catherine Gebotys, "A Quantitative Analysis of a Novel SEU-Resistant SHA-2 and HMAC Architecture for Space Missions Security" *IEEE Transactions on Aerospace and Electronic Systems*, Vol.49,No.3 2013, pp.1536 – 1554.
[9]. Matthias Strobbe et al., "Implementation and evaluation of AntNet, a distributed shortest-path algorithm" *IEEE* 2005, pp.320 – 325
[10]. Robert Leidenfrost and Wilfried Elmenreich, "Establishing Wireless Time-

Triggered Communication using a Firefly Clock Synchronization Approach" *IEEE Xplore*, 2009

[11]. Sung-Ju Lee, et al., "A Simulation Study of Table-Driven and On-Demand Routing Protocols for Mobile Ad Hoc Networks" *IEEE Network*, 1999, pp.48-54.

[12]. Leidenfrost, "Establishing Wireless Time-Triggered Communication using a Firefly Clock Synchronization Approach", *Proceedings of International workshop on Intelligent solutions in embedded systems (WISES'08) 2008*, pp.227 – 244.

[13]. Ramkumar. K.R, Ravichandran, et al., "SACOM: Secure Ant Colony Optimization for MANETs" *International Journal of Computer and Electrical Engineering*, Vol. 1, No. 2, 2009, pp.164-169.

[14]. Bing Wu et al., "A survey of attacks and countermeasures in Mobile Adhoc Networks" *Wireless/Mobile Network Security*, Springer 2006

[15]. 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*, ISSN 1947 5500, Vol.4,No.1&2, 2009,.

[16]. Priyanka Goyal et al., "A Literature Review of Security Attack in Mobile Ad-hoc Networks" *International Journal of Computer Applications,* ISSN -0975-8887, Vol.9, No.12, 2010, pp.11-15.

[17]. Jamal Raiyn, "A survey of Cyber Attack Detection Strategies", *International Journal of Security and Its Applications*, ISSN: 1738-9976 Vol.8, No.1 (2014), pp.247-256.

[18]. Shailendra Singh and Sanjay Silakari, "A survey of cyber attack detection systems" *International Journal of Computer Science and Network Security*, Vol.9 No.5, 2009, pp.1-10

[19]. Frederick T.Sheldon and Claire Vishik, "Moving Towards Trustworthy Systems: R&D Essentials" *IEEE computer society*, 2010, pp.31 – 40.

[20]. L.M.Hively et al., "A vision for Scalable Trustworthy Computing" *IEEE Security and Privacy, ISSN. 1540-7993,*

Biographies

M. Uma is a Ph.D. research scholar of Avinashilingam 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 department of Avinashilingam University for women, Coimbatore. She has 25 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. Presently she is guiding M.phil researcher and PhD Scholars. 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 the scientific mentor for one project funded by DST. She is life member of many preferred organizations of CSI, ISTE, WSEAS, AACE, and ACRS.