ISSN 2047-3338

An Intelligent Distributed Reputation Based Mobile Intrusion Detection System

Dr. S. Madhavi[1] and Dr. Tai Hoon Kim[2]
[1]Department of CSE, Affiliated to JNTUK, India
[2]Department of CSE, Hannam University, Korea

***Abstract*—The communication channel in Mobile Adhoc Networks is shared among the nodes in the network and the MAC layer plays an important role. Many attackers try to affect the features of Physical, Network or MAC layers. Also the dynamic nature of the Mobile Adhoc Networks and the lack of centralized control demand an intrusion detection system suitable for the MAC layer. In this paper, we propose an Intelligent Distributed Reputation based Mobile Intrusion Detection System, to detect the malicious node so as to improve the system throughput.**

***Index Terms*— MAC, SOM, DoS, U2R, IDS and IRmIDS**

I. Intrusion Detection Systems

SECURITY for Mobile Ad-Hoc Networks is becoming an attractive challenge for many researchers. Today's firewalls and encryption software's are not sufficient and effective to protect networks. In Mobile Adhoc Networks there is no centralized control and hence a detection system is needed. A Simplified Clustering Scheme for Intrusion Detection in Mobile Ad Hoc Networks is proposed by Kashan Samad, Ejaz Ahmed, Waqar Mahmood. AikateriniMitrokotsa, Rosa Mavropodi, Christos Douligeris proposed an Intrusion Detection of Packet Dropping Attacks in Mobile Ad-Hoc Networks. D.B. Johnson and D.A. Maltz proposed a Dynamic Source Routing in Ad-Hoc Wireless Networks. S. Marti proposed a Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks. H. Yang, X. Meng, and S. Lu proposed a Self-Organized Network Layer Security in Mobile Ad Hoc Networks. J. Kong proposed a paper on Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks. K. BAL Krishnan, J. Deng, P. K. Varhney proposed a TWOACK: Preventing Selfishness in Mobile Ad-Hoc Networks.

Here we propose a new IRmIDS suitable for Mobile Adhoc Wireless Networks which detects nodes misbehavior, anomalies in packet forwarding, such as intermediate nodes dropping or delaying packets. IRmIDS does rely on overhearing packet transmissions of neighboring nodes. Simple rules are designed to identify the misbehavior nodes. Intrusion detection is the process of monitoring and analyzing events that occur in a computer or networked computer system to detect the behavior of the users that conflict with the intended use of the system. Attacks in MANETs can be classified as Passive attack, Active attack, Network Layer Attack, Transport Layer Attack, Application Layer Attack and Multi Layer Attack.

The following are various performance metrics used in IRmIDS:

- True positive rate (TPR) = $\frac{TP}{(TP+FN)}$

  Classifying an intrusion as an intrusion

- False positive rate (FPR) = $\frac{FP}{(TN+FP)}$

  Incorrectly classifying normal data as an intrusion

- True negative rate (TNR) = $\frac{TN}{(TN+FP)}$

  Correctly classifying normal data as normal

- False negative rate(FNR) = $\frac{FN}{(TP+FN)}$

  Incorrectly classifying an intrusion as normal

- Detection rate = $\frac{(TP+FN)}{TP}$
- False Alarm Rate = $\frac{(FN+TP)}{FN}$

II. PROPOSED WORK

A. Introduction to IRmIDS

In our earlier paper (Madhavi and Kim 2008) a hierarchical architecture is assumed where nodes in the networks can become heads of clusters of nodes. The cluster heads detects

the malicious nodes in the cluster and also locates and determines Byzantine nodes. But the procedure of creating clusters and electing cluster heads creates an extra overhead on the processor and hence the performance of the system may be decreased. Hence in our next paper (Madhavi and Kim 2009) the mIDS runs in each node and makes the decisions to detect the malicious nodes. Each node in the wireless ad hoc network uses the neighbor's data to identify the malicious node. A threshold method is used to limit the risk created by malicious nodes. In our next paper (Madhavi and Ramesh 2009), we proved that our proposed mIDS minimizes control overhead and maximizes the network throughput. In our next paper (Madhavi and Ramesh 2010) we proved that the performance of our proposed mIDS outperforms the other existing work on Mobile IDS.

In this paper we propose a response system based on several mobile IDS agents for detecting different malicious activities in a node. These multiple IDS agents called IRmIDSAGENTs detect and locate the malicious nodes. The IRmIDSAGENT builds its own data from the local neighborhood. From this data it constructs the information about the entire network. Each IRmIDSAGENT continuously overhears the neighbor nodes activities. Each mobile node transmits its packet with the control data embedded in it. This data is used by the proposed algorithm for detecting the malicious node. The node is not punished in our system; instead the node is sending multiple ALERTS about its malicious activities. And if these reminders reach a certain threshold, the malicious node is simply ignored by the remaining nodes in the network.

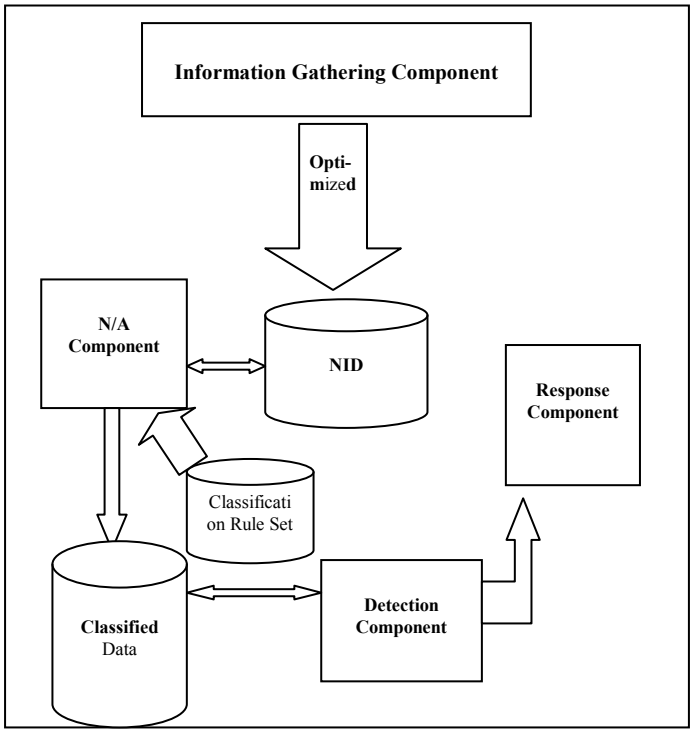

Fig. 1: Components in an IRmIDS agent

Each local IRmIDS agent is composed of the following components.

1) Information Gathering Component: The IGC is responsible for gathering the local neighborhood. Each node constructs the global data from this local data. For example,
Let node b and node c are the 1-hop neighbors and 2-hop neighbors of node p.

Let node d and node c are 1-hop and 2-hop neighbors of node q.

Let node p and node q are 1-hop and 2-hop neighbors of node r.

From the local information node r understands that nodes p , q are its 1-hop neighbors
Nodes b is its 2-hop neighbors
Nodes d, c are is its 3-hop neighbor.

Since the mobile adhoc networks lacks centralized control the local and global data is maintained by each node. Whenever there are topological changes the information about the entire network is rebuild by each node in the network. We used optimization techniques so as to minimize the size of this data. A copy of this optimized data is stored in NeighborInfoDatabase.

2) The Neighbor Info Database: The NID is the optimized data that contains all the information necessary for the IRmIDS agent, such as the neighbors control information.

3) N/A Component: The N/A component computes the level of dissimilarity using the gathered controlled data and the store data and classification rules. The classification rules are simple IF-THEN rules. The returned dissimilarity level is used in the proposed algorithm to test and classify a node as Normal or Abnormal. The dissimilarity level and the classified data are updated in CNID classified neighborhood database for the future analyses. Even a minute dissimilarity is noted and the necessity for that small change is also analyzed.

For example;
Let X is a node in the network
Let a , b , c are 1-hop neighbors of X

CLASSIFICATION RULE1

IF ((level=increase_in_trans_speed (of a neighbor X)) > 0)
THEN

a. If receivingcapacity((1-hop neighbors of (X 's 1-hop neighbor nodes)) < sendingspeedof(X's 1-hop neighbors)
// nodes will drop packets (flow control problem)
then report as malicious activity, ABNORMAL
Else
report NORMAL
endif

b. If there is an remarkable increase in receiving capacity of X's neighbor so as to achieve high data rates

```
        then
              report as NORMAL
        else
             report as ABNORMAL
        endif
Endif
```

CLASSIFICATION RULE2

```
If ( (level=Cmp(neighbor_list[a],Global_data[X])) > 0 )
// If any deviation
   Report as malicious activity, ABNORMAL
Endif
```

CLASSIFICATION RULE3

If X receives a packet in a slot not currently belong to any of its 1-hop neighbors then

a. Verify the source address
b. Call it as malicious node
c. Report malicious activity , ABNORMAL

Endif

The current dissimilarity level is also compared with the stored n number of previous levels. A gradual increase or decrease in these levels without any noted reason is also considered as an abnormal behavior.

4) Detector Component: The DC on each mobile IRmIDS agent monitors constantly to detect and locate the malicious node. The ABNORMAL nodes data is collected from the classified database. Depending on the type of the abnormality the various parameters like user input speed, how much of time passed between the Receptions of two consecutive messages, how many number of messages are transmitted or received by the neighbors, whether any collisions are detected in the network, whether the nodes are following the broadcast schedule etc are observed. Sometimes a node's abnormality is due to its neighbor's malicious activities. Hence a local DC may also contact neighbor nodes DC for any global data required for detection of anomalies. From this global contact the location of the malicious node also can be identified.

5) Response Component: The Response Component is responsible for sending alerts to all the nodes in the network about the attack type. Also the malicious node is warned about its malicious activities. If the malicious node does not stop its activities after a certain period of time (threshold limit) the malicious node is declared as IGNOREDNODE and this information is broadcasted to all the nodes in the network. From then the nodes in the network simply ignores the activities of the IGNOREDNODE i.e. neither the data is not sent to it nor received from it. Sometimes the response may be even to send signals to IGNORENODE to shut down the node.

B. Proposed IRmIDS Algorithm

IRmIDS(IRmIDSAGENT)

//Each IRmIDS agent executes the algorithm to classify the data as Normal or Abnormal.

//Afterwards IRmIDSAGENT detects the Intrusion type and also the Malicious Node.

NID Neighborhood Intrusion Database
mIDS Mobile Intrusion Detection System
CBS CurrentBroadcastSchedule
N Size of the Neighborhood data collected by the local IRmIDSAGENT
CNID Classified NeighborhoodDatabase
Responsethreshold a larger value where after the node is punished

```
struct   Neighborhood_Info
{
   List            *NeighborId
   Power           *PowerInfo
   Threshold       *PowerThres
   Capacity        *Receivingcapacity , *SenderCapacity
   Speed           *TransSpeed , *ProcessSpeed
   Delay           *Transdelay ,* ProcessDelay , *RecevDelay
   Int             *NoOfRecvPackets, *NoOfSendPackets,
                   *NoOfProcessPackets
   Schedule        *CurrentSlot
   Length          *RecvMesgLen,      *SendMesgLen
            ,      *RMaxLen,*SMaxLen
   Ratio           Packet delivery ratio
   Time            Network joining time
   int             NoofActiveneighbornode                ,
Spatialreuse
            ,      Noofneighbors
   SEQNO           *Seqnoatneigh
   Buffer          *Recvbuff,          *Sendbuff
   Int             *Transmissionrange , *Responselevel
   Rate            *Datarate
   }
```

1.0 Construct the Neighborhood_Info(IRmIDSAGENT)

//This record is constructed from the neighbors who are reachable from the local mIDS agent

2.0 Import CurrentBroadcastSchedule
3.0 GET CurrentSlot[IRmIDSAGENT] from CurrentBroadcastSchedule
4.0 UPDATE NID = OPTIMIZE(Neighborhood_info, N,IRmIDSAGENT)

//The multiple mIDS agents from their Neighborhood_info
5.0 constructs optimal Data
6.0. If (SIGNAL(NID,IRmIDSAGENT)) = S_ABNORMAL

```
)
    then
     (MaliciousNode,IntrusionType)  =
    DETECTCMPNT(CNID.IRmIDSAGENT)
     Response_level=RESPCMPNT (MaliciousNode ,
                                          IntrusionType)
7.0. End
```

SIGNAL(NID,IRmIDSAGENT)

```
// IRmIDSAGENT analyzes the database and classifies a node
//as either ABNORMAL or NORMAL
//Each IRmIDSAGENT maintains a recvbuff which contains
a //copy of the last OLD number of packets from all its 1-hop
//neighbors.
//Various Classification Rules are applied on this control
//portion of these packets for classifying the node.

1.0. For mIDSNEIGH in { List of 1-hop /2-hop neighbors of
     IRmIDSAGENT]
     do
      UpdateStrdpckts=Control_pkts(mIDSNEIGH,Recvbuff)
      Dissim_level=Classify(mIDSNEIGH , Strdpckts ,
                                ClassifyRuleSet)
      If   Disssim_level = RISK
           Update  CNID
            REPORT     S_ABNORMAL
      Else

      if    Dissim_level = SAFE
           Signal          S_NORMAL
      Endif
2.0. Stop
```

DETECTCMPNT(CNID,IRmIDSAGENT)

```
//mIDSNEIGH denotes the 1-hop/2-hop neighbors of
IRmIDSAGENT
// multiple mIDS AGENTS exits and they continually monitor
//to detect a different type of anomaly
// If IRmIDSAGENT could not categorize the ABNORMAL
//node into any of its known attacks it is placed in an
//UNKNOWN_ATTACK category.

1.0. For all mIDSNEIGH in {List of 1-hop/ 2-hop neighbors
     of IRmIDSAGENT}
   do
```

- **PACKETDROPPINAGENT**

```
   START
        DIFFERENCE(NoOfRecvPackets , NoOfSendPackets
                        , mIDSNEIGH)>0
        or
        (ProcessDelay < Processdelaythresh )
           REPORT Packet Dropping.
        If packets are dropped according to some specific criteria
        then
              REPORT selective dropping / gray hole attack
        END
```

- **COLLISION/BYZANTINEAGENT**

```
   START
     NBELONG( CurrentSlot , CurrentBroadcastSchedule ,
                  mIDSNEIGH)
                   REPORT Collision  ,Byzantine Attack
   END.
```

- **BANDWIDTH_ResourceConsumptionAGENT**

```
   START
     if DIFFERENCE ( spatialreuse , CSES_notimestrans ,
                              mIDSNEIGH )  >  0
   Or
     If(DIFFERENCE ( spatialreuse, NoOfRecvPackets) > 0
      REPORT BANDWIDTH_ResourceConsumption Attack
   END
```

- **HIJACKINGAGENT**

```
   START.
    COMPARE (   GET(Seqnoatneigh,mIDSNEIGH),
   GETNEIGH(Seqnoatneigh,noneighbors,      mIDSNEIGH))
>0
   REPORT Hijacking.
   END
```

- **DENIAL OF SERVICEAGENT**

```
   START
(COMPARE (   GET(Seqnoatneigh,mIDSNEIGH),
 GETNEIGH(Seqnoatneigh,noneighbors,mIDSNEIGH))<=  0
)

   And
    (NBELONG ( CurrentSlot , CurrentBroadcastSchedule ,
                  mIDSNEIGH)
          REPORT Denial of service.
   END
```

- **JAMMINGAGENT**

```
   START
   ( DIFFERENCE ( Spatialreuse , CSESH_notimestrans ,
                  mIDSNEIGH) <= 0
   or
   DIFFERENCE(Spatialreuse, NoOfRecvPackets) <= 0 )
   And
    ((DIFFERENCENEIG(Spatialreuse                    ,
CSESH_notimestrans
                  , noneighbors,mIDSNEIGH)<= 0)
    Or
   DIFFERENCENEIG ( Spatialreuse , Noneighbors ,
                              NoOfRecvPackets) <= 0 ) )
          REPORT Jamming.
```

END

- **FLOODINGAGENT**

START
DIFFERENCE (Receivingcapacity , mIDSNEIGH, NoOfSendPackets) > 0
Or
Intervelbetween (SendPacket,ProcessThreshold,mIDSNEIGH) > 0
REPORT Flooding.
END

2.0. END

RESPCMPNT (MaliciousNode, IntrusionType)
// MaliciousNode denotes the node which carries malicious activities
//All the other nodes in the network are informed to simply ignore
//the activities of the malicious node
// CMAX_hop is set to the current maximum hop of the network

1. Increment responselevel of MaliciousNode
2. If responselevel > responsethreshold

   a. CREATE (ALERT = IGNORE_Node , Message = IntrusionType)
   b. SETUP FLODDING_ALARM with CMAX_hop value
   c. BROADCAST ALERT

   //Each node in their turn to Broadcast , sends ALERT to its neighbors
   //this happens until the FLODDING_ALARM is reset

3. Stop

III. RESULTS

The IRmIDS is executed using a network consisting of 20, 40, 60 80 100 number of nodes. Any TDMA scheduling method may be used to find an efficient scheduling method for all the nodes in the Mobile Adhoc Network. A transmission range of 150m with the distance between the nodes as 50m is assumed in a denser area than in [14]. The IRmIDS is tested with the number of malicious nodes as 0,5,10,15,20,25 ,30,35,40,45 and 50.

It is observed that malicious node is always identified as ABNORMAL by the N/A component and categorized into an appropriate ATTACK type by the detection component. But sometimes when a node changes its identity remarkably without any cause, and if there are any system /network/unknown problems , then there is a probability for IRmIDS to falsely identify it as an ABNORMAL node and placed into an UNKNOWN_ATTACK type. This happens very rarely for whenever network / system / unknown problems arises in the network.

Hence in our experiments
The True positive rate TPR is always 100%
The False positive rate FPR is between (90-100) %
The True negative rate TNR is between (90-100) %
The False negative rate FNR is always 100%

IV. CONCLUSION

The metrics like TPR, FPR, TNR and FNR are calculated. Usually the most effective approach should reduce the False alarm rate and increase the Detection rate. Since on each recital of the packets the node verifies for an intruder, the probability for not detecting malicious node is very rate. The detection rate is high when compared with the other existing methods like in reference number 14. The false alarm rate of IRmIDS is considerably less when compared with the other existing methods. The complexity of IRmIDS procedure is very less. There are no clusters and hence no extra overhead for cluster management. Also control packets are not used for maintaining the network intrusion detection system. But each node allocates some space (less than 5% of the overall packet data) for control data in each packet.

Since the amount of space occupied by the control portion is negligible (less than 5%) in each packet the throughput of the system is more with IRmIDS. In all the existing methods the control overhead (due to cluster management, detection system management) is smaller when the total numbers of nodes are less (50) and larger if the number of nodes are more (100). In IRmIDS the control overhead do not depend on the number of nodes. Hence on an average the control overhead is negligible with IRmIDS when compared with the other existing methods for intrusion detection in mobile adhoc networks at MAC level. Since the nodes do not separately transmit the control packets, all the transmission slots are solely used for the transmission of packets itself, there is a considerable improvement in system throughput with IRmIDS.

REFERENCES

[1] S.Madhavi and I.Ramesh Babu "Security for Mobile Adhoc Networks Challenges and Solutions", Journal of Computer Science, Karpagam, Vol. 1, Issue 6, Sept-Oct 2007.

[2] S. Madhavi and Tai-hoon Kim, "An Intrusion Detecting System in Mobile AdHoc Netwoks", International Journal of Security and its Applications, Vol. 2, No. 3, July 2008.

[3] S. Madhavi, "An Intrusion Detecting System for Mobile AdHoc Networks", Indexed in IEEE Digital Xplore conference proceedings of ISA, April 2008.

[4] S. Madhavi and Lakshmi, "Anti-Phishing System to Detect Phishing Web Pages with Visual Similarity Assessment", International Journal on Computer Engg & Information Technology (IJCEIT), ISSN 0974-2034, pp. 3-21, Vol. 3, No 4, March 2009.

[5] S. Madhavi and I. Ramesh Babu, "Maximizing the Throughput in Mobile Adhoc Networks", International Journal CIIT, November 2009.

[6] S. Madhavi, Tai-hoon Kim, Julian Dermoudy and Byeong-Ho KANG, "A Reputation Intrusion Detection system in Mobile Adhoc Networks using a Set Based Election Monitior

Protocol", Masaum International Journal of Computing, Vol. 1, No 1, August 2009.
[7] S. Madhavi and Vijaya, "Authentication of People Based on Typing Pattern with Artificial neural Networks", International Journal on Computer Engineering and Information Technology (IJCEIT), ISSN 0974-2034, pp. 94-101, Vol. 5, No. 8, March 2009.
[8] S. Madhavi and I. Ramesh Babu,"Performance analysis on mIDS", Acharya Nagarjuna University International Journal of Engineering & Technology, Vol. 1, No. 1, pp. 1-7, June 2010.
[9] S. Madhavi, "Long Term Security for Signed Documents", in the Proceedings of NEXTGENERATION IT, an International Conference, at Sri Satya SaiBaba Institute at Prasanthi Nilayam Ananthapur, 2006.
[10] S. Madhavi, "A new Intrusion Detection System for Mobile Adhoc Networks", in the Proceedings of a National Conference organized by V.R. Siddhartha College of Engineering, 2007.
[11] S. Madhavi, "Security for Mobile Adhoc Networks: Challenges and Solutions", in the proceedings of a National Conference organized by V.R. Siddhartha College of Engineering, 2007.
[12] Y. Zhang and W. Lee and Y. Huang. Intrusion detection techniques for mobile wireless networks. In ACM/Kluwer Mobile Networks and Applications (MONET), Vol. 8, pp. 545– 556, Sep 2003.
[13] Kashan Samad, Ejaz Ahmed, Waqar Mahmood, "Simplified Clustering Scheme for Intrusion Detection in Mobile Ad Hoc Networks", 13th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, September 15-17, 2005.
[14] Aikaterini Mitrokotsa, Rosa Mavropodi, Christos Douligeris, "Intrusion Detection of Packet Dropping Attacks inMobile Ad Hoc Networks", International Conference on Intelligent Systems And Computing: Theory And Applications, Ayia Napa, Cyprus, July 6-7, 2006.
[15] D.B. Johnson and D.A. Maltz. Dynamic Source Routing in Ad-hoc Wireless Networks, Chapter 5, pp. 153–181, 1996.
[16] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", ACM MOBICOM, 2000.
[17] H. Yang, X. Meng, and S. Lu, "Self-Organized Network Layer Security in Mobile Ad Hoc Networks," ACM Wise, 2002.
[18] J. Kong et al., "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," IEEE ICNP, 2001.
[19] K. BAL Krishnan, J. Deng, P. K. Varhney. TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks. In IEEE WCNC, March 2005.

Dr. S. Madhavi received her M.S. Degree in Software Systems from B.I.T.S Pilani and Ph.D. in Computer Science and Engineering from Acharya Nagarjuna University. She is presently working as a Professor, in the Department of Computer Science and Engineering, affiliated to Jawaharlal Nehru Technological University, Kakinada. She has guided 40 postgraduate student projects. She has Published 16 papers (International & National Journals / Intl Conference proceedings) and had Academic Participation in 11 International workshops / conferences. She is a member of advisory/Editorial Board of Masaum International journal of Basic Sciences and Engineering, Masaum International Journal of Computing, and SERC- International Journal of Applied Sciences and Technology and SCICON. Also a life member in Computer society of India and ISTE . She is also a member of IAENG . Her areas of interest are Network security, Wireless Networks, Network protocols, Mobile computing, Artificial Intelligence and Neural Networks.

Dr. Tai Hoon Kim received his M.S. Degree and Ph.D. in Electrics, Electronics & Computer Engineering from the Sungkyunkwan University, Korea. He worked as researcher at Technical Institute of Shindoricoh, as a senior researcher at the Korea Information Security Agency, at the DSC (Defense Security Command), as a research professor at E-wha Woman University and now he is currently a professor of Hannam University. He wrote sixteen books about the software development, OS such as Linux and Windows 2000, and computer hacking & security. And he published about 150 papers by 2007. He was a General Chair of ICHIT 2006, MUE 2007 and ISA 2008 , Steering Committee Chair of FBIT 2007, IPC 2007, FGCN 2007 and MUE 2008, and Publicity Chair of JRS 2007. Now he is a Steering Committee Chair of FGCN 2008, ASEA 2008, SecTech 2008, BSBT 2008 and UNESST 2008. He was a Guest Editor of AJIT and FGCS Journal.