RGB Technique of Intrusion Detection in IEEE 802.11 Wireless Mesh Networks

M Salman Ashraf[1] and Muhammad Raheel[2]

[1]Department of Computer Science
University Of Central Punjab,
Lahore, Pakistan

[2]Department of Computer Science
University Of Central Punjab,
Lahore, Pakistan

Abstract

According to the growth rate of wireless technology, wireless mesh network (WMN) usage is significantly increased according to its advantages like inexpensive, fast and easy deployment. WMN have ability, easy to create mesh and provide internet access in a cost efficient manner in any type of area which is unable or costly for wire mediums. Security attacks ratio is higher in wireless mesh network (WMN) rather than other wireless or wire technologies. Spy /Malware infected computers generate malicious traffic, which uses valuable network resources and puts other systems at risk. Intrusion detection system (IDS) is one of the possible solutions which timely detect the intrusions and alarm for appropriate action. But Limitation of many IDS of WMN are not timely response or unable to share with all nodes due its dynamic network topology and easy access to the radio medium. In this paper, proposed framework is timely detect intrusion and in response to share with all, in both standalone and cooperative manner. This paper also provides the basic sharing mechanism of intrusion for large scale bandwidth wireless mesh networks.

Keywords: *RGB, Wireless mesh network, intrusion detection, and security.*

1. Review of Intrusion Detection Systems for WMN:

Internet is necessary element consider for many purpose like business today. People need any type of medium to connect internet but many areas including develop cities may not have broadband infrastructure or high quality cable .QoS, upgrading makes high expensive for largest ISPs or its related companies. The ratio of WMNs growth, several companies realize features of WMNs as a low cast internet access solution and produce broad range coverage in any type of area. However, still it is one of the most important research issues 'security' in multi-hop wireless networks such as IEEE 802.11 WMN and MANET.

In WMNs, several ways to sending and receiving data packets in cooperative mesh nodes. Rising the WMNs security issue, intrusion detection is measured in terms of false positives and false negatives.

Intrusion detection systems attempt to minimize both statistics. But intelligent attackers can try to evade these detections which are purposed for MANET environment, is fully explained in [1].

One of the earliest intrusion detection schemes proposed for the Internet environment was 'WATCHERS'. Watchers are monitoring in distributed or decentralize network, use for watch the evidence of false node or anomalies or remove from network and keep the log files and counts of all the routers in link state routing protocol. The counter values of passing packets are analyzed between neighbors or node which is cooperating to find anomalies on every node as independently observing their neighbors. It use in decentralized nature, node totally independent to check the incoming packets , detect anomalies and track the counter value of data going through neighbors node. The counter value is miss-routed packets which are based on share information from neighbors' routing tables. The objective is to find out anomalies in distributed way. Watchdogs and pathraters [2] are purpose for Intrusion detection and use for type of DSR routing protocol to detect anomalies. Watchdog monitors the neighbor's behavior, while pathrater monitor the watchdog data, and select best path for packet delivery. Each router checks incoming packets to detect any routing anomalies.

Nodes/Routers are flooding their statistics in network to start the diagnostic phase. Due to data sharing nodes are independently act to find out the malicious /false nodes that might try to interfere in the sharing. But theses scheme is not detect invisible node attacks below some threshold. In TIARA [3] method are used to find out the path failure, and sending the message about the path, which increases its cost. CONFIDANT [4] method monitor and assign the values for behavior of its neighbors, and raises an alarm if intrusion come. If a router/node is found in any of these misbehaviors, it assigns to as bad router. But it is

difficult to determine about router/node external behavior when intrusion acts. Mobile Intrusion Detection System (MobIDS)[13] are used to find out groping packet node and classify in cooperative or non-cooperative node and broadcast to neighbors but it can't differ between malicious node and power failure node. AODVSTAT [5, 6] is a routing protocol use in sensors which sense the attack in neighbors by sharing in two different modes; 'ADOV' is an extension of STAT protocol method which use signature based detection method to find out intrusion by snapshot of host memory which is dividing in three classifications [7]. ADOV method request for routing path from source to destination, if reply by intermediate malicious /false node then AOVSTAT sense that node. But not define how to update attacker signature file in all mesh nodes of MANET. The RESANE and SCAN [8] method are used to make statistics about behavior of node/router and motivate the bad node to list in cooperative node by good behavior throughout the network. If the node continues misbehavior, its statistics flooding continue which show its reputation the node will become isolated from the network. Flooding statistics is observed by neighbors to calculate its reputation of node. Then neighbors broadcast to other for help them, protect themselves. Thus, the overall network is protected by cooperative information sharing. SCAN [8] method tells us about routing only. Packet forwarding misbehavior [9] is that routing decision depends on internal node/router which is the part of network, whereas Packet forwarding misbehavior is externally interfaces [8, 9] e.g. packet dropping, packet misrouting. However it is depend on AODV routing protocol. In [11, 10], the method proposed of distributed IDS for mobile nodes. But these are static in ieee802.11. In [10], a rule base method of IDS is not able to find out unknown attacks.

2. Introduction:

Due to all of earliest purposed methods/techniques have some limitations which are consider importantly in RGB framework of intrusion detection system. RGB (red, green and black database) method is depend on database sharing. Limitation in above methods is mostly about depend on protocol, less memory, unable to update whole nodes in network and differentiates between power failure node behavior and malicious node which initiate intrusion. Remember objective is detecting intrusion. This framework works according to some rules of share the chunks of these three databases between nodes.

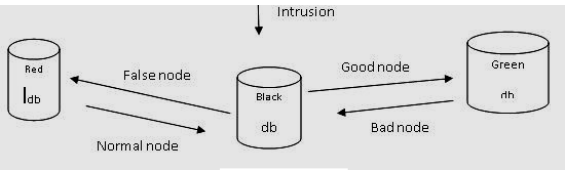

Fig 1.1

Databases which are in this framework are red, green and black database. Red database consist of name of those nodes which have bad behavior or detect in produce intrusion. Green database consist on those nodes which have good behavior or cooperative node or not include in any packet dropping misbehavior. Black database consist on all new entry nodes which wants to communicate with other.

2.1. Classification and Component of IDS:

Generally IDS works are dividing in two group hold. Pattern Base IDS are used to detect all those intrusions which are known or use before. Anomaly Base IDS are used to detect all those intrusions which are not known or not use before. According to node, there are 3 types of IDS which are Stand-alone IDS: to operate on each node independently, monitor all events and make database. Cooperative and distributed IDS: to operate on share information rule between all nodes and make database on all participating nodes in network and response. Hierarchical: to operate on all child nodes or new nodes and only response in the case of intrusion [12, 11].

Any IDS have two parts, features and algorithms. Algorithms are a core component design on the rules and produce features. Features are the combination of facilities and output of the particular algorithms. Previously describe in review section, all-purpose IDS have some common components which are:

Monitoring: use to monitor the nodes, neighbors or itself. Database or log file: use to record event by intrusion effect, make statistics and share with other nodes. Response: after intrusion detect, what system or node can do in reply or response. One of common response is rise Alarm, whereas broadcasting information to neighbors or flooding these DBs or log file in to entire network nodes.

However the algorithm nature is mostly affected in common components because of base rules and response nature. Like one of IDS response in term of flooding information of intrusion base node in all network to make independently statistics or database. Some of IDS have common monitoring system at physical of Mac layer intrusion. Whereas some of IDS work on make layer by layer log files or Databases and in response to share.

2.2. Limitation & issue of IDS:

IDS design have these issue;

- WMN have fix infrastructure about nodes/ routers/gateways that's way power limitation is not issue.
- WMN can support any other wireless technology to merge.

- WMN have no computational or memory limitations.
- WMN traffic flow to or from gateway through radio access points which have fixe and not have power issue.
- Every node/ router connects to every other to create mesh.

Some limitations are:

- Intrusion node information is not share between all nodes/routers of exiting network.
- Nodes Misbehaving are in same list of malicious nodes.
- Power failure nodes and data packet drop nodes are not differentiating.
- Have no rule between sharing and flood information in all nodes.

RGB technique is purpose for remove the limitation and work in any central or decentralized nature of WMN. This technique produce result based on sharing rules between routers/nodes due to any intrusion detect by any system.

3. RGB:

RGB framework is design to cover all limitation of existing IDS at large scale multi-hope WMN with independently as node and cooperatively as mesh router. RGB have two level of work at cross layer which are one of is as front level and second is backbone level.

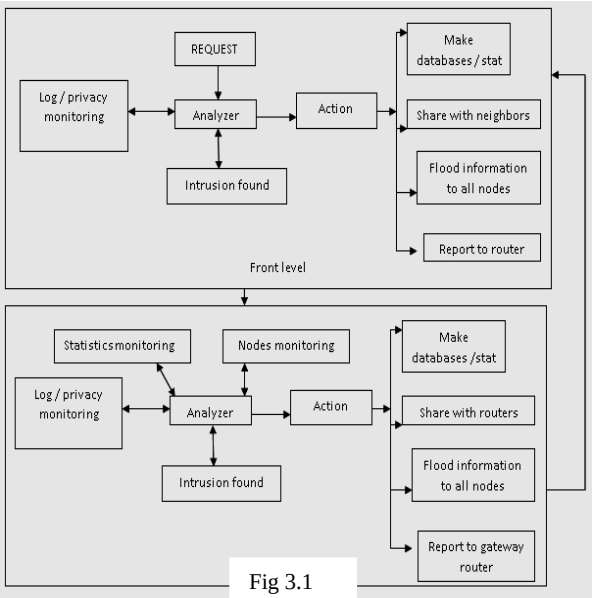

Fig 3.1

Front level deal with nodes which are connect with routers and work as independently to make RGB Databases to prevent its neighbors and itself with its router network. Front level also deals with cooperative sharing node to other network nodes.

Backbone level is deal with mesh routers to make RGB databases and inform each other routers in existing network. Backbone level also deal with gateway mesh routers which are important component between inner and outer source network.

The purposed IDS technique works at the rule of RGB databases and will meet all security requirements and improve the quality in future prevention using additional databases. In this two cooperative level of IDS, the nodes are monitoring cooperatively and independently. When intrusion found, both level establish and work together which perform better result to make and share RGB databases. These phases and databases are following describe.

3.1. Monitoring Phase:

Monitoring phase are divide in two parts and its working describe are:

1. **Front level monitoring :**

In which each node monitor its neighbors as independently like other IDS which are describe in Reference. Every request from any nodes/ router is analyze if it has to access log file or privacy than particular node will made 4 type of action which are in fig3.1 .

1. Make RGB database as independently and cooperatively by confirmation of its neighbors.
2. Share latest chunk of whole RGB data bases with neighbors and routers.
3. Flood only RED database as whole to all nodes. RED database always establish by cooperative communication not standalone position.
4. When ever found any misbehavior of node by its statistics which are record in databases or intrusion generator node founded than node report to its network mesh routers.

2. **Backbone level monitoring:**

In which network mesh routers investigate on more than two same reports from different nodes in its network. it analyze nodes statistic by providing from nodes in RGB databases and monitor node behaviors as individually by establish directly connection with that particular node. If node is an intrusion or misbehavior node than RGB IDS makes an action in fig 3.1 against particular node. If router is involve to generate intrusion or in packet drooping misbehaviors than router will report to gateway router and make same 4 type actions against that particular router.

1. Make RGB databases/ statistics as cooperatively by network mesh routers and nodes.
2. Share latest chunks of databases to other mesh routers
3. Flood RGB databases to all network nodes. Only RED database flood at fixe time interval in to network. Other database latest chunks are broadcasting in entire network.
4. Whenever RED database entry make than report to gateway routers.

3.2. Database and Response Phase:

3.2.1. RED database:

Red database consist of false/ malicious nodes / routers. These nodes come from the black databases of nodes which make it as independently or cooperatively share between mesh routers or nodes to find a false node /router which want to access the privacy of any individual node or set of nodes. RED DB also has those nodes which have low statistic about its performance.

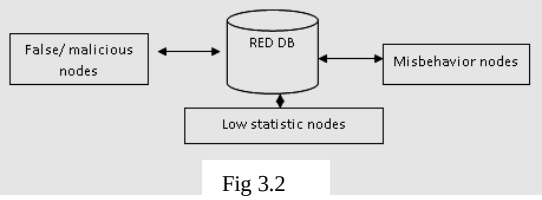

Fig 3.2

False nodes are those nodes which generate intrusion or involve to access log files or privacy of any node. Low statistic nodes are those nodes which are involve in packet dropping. Misbehavior nodes are type of low statistic node but it is differ from the power failure nodes which are not answering after power failure.

Red DB is not to make as independently or at own position as node. It make by cooperatively approach in WMN. Whenever intrusion found by any individual node-A, it put in Black DB but when again and again found intrusion from same node, the node-A make entry from black DB to Red DB and share with neighbors. Neighbors investigate the particular node by its behavior. Neighbors invite particular node to make connectivity directly and sharing. If this particular node is try to access privacy of neighbor's node. The neighbor's node sure that is a false/ malicious node, break connectivity with that and broadcast to its own neighbors which node-A is also get confirmation by its neighbors broadcast. it's make throw sharing and make whole database share with neighbor and only flood latest information in entire network. So Red DB always makes by neighbors "cooperatively approach" in WMN.

$\sum i = (\sum pri + \sum psi) / \sum pdi$ where $pr \geq pd$

Example:

Pr=500 pd=100 ps=pr-pd=400 at ith time =10mili so $\sum i=9$

ps value depends on receiver of nodeA. pr value depend on sender node A. ith is a time line and pd value is dropping packets at nodeA.

Fig 3.4

- No of receiving data packets *pr*
- No of data packets sending *ps*
- No of data packet dropping *pd*

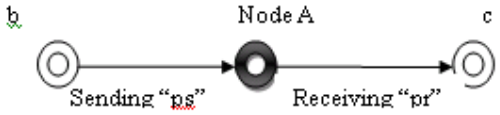

Fig 3.5

Red Database Table

NODs	Status	Time stamp (sec) max=10000	Statistics > threshold 500
node 2	Live	0	614
node 8	Invisible	14	null
node 15	Dead	Null	532

Fig3.3

In fig3.3, live mean node is in position to generate intrusion and invisible mean when no connectivity hole with particular node than no activity shows by particular node and its time stamp is continue if during the time it is active/ visible than its status look like node 2 in fig 3.3 else if time greater than maximum, this node will remove from red DB and put in to black

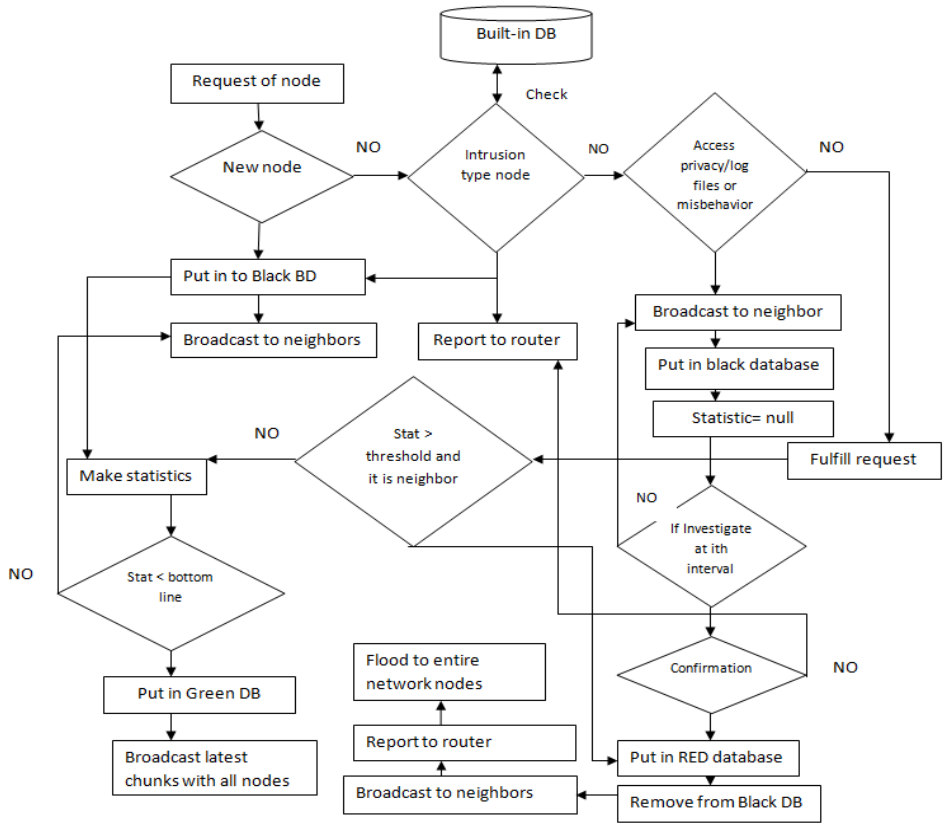

Fig 3.7

DB. Dead status nodes are those which are block in entire network , no one is communicating to that node or listening its request. This type of node is made from node 2 type and its timestamp is goes to null until it is not generate intrusion. Whenever it is stop to generate intrusion, by their statistics which show its performance than timestamp is active but during timestamp, node remains in Red DB. No request will be listening of all those nodes which are in this database, its uses only for forwarding data packets to other or make path between nodes. If its statistic going positive/ lower than node timestamp is goes maximum and this node remove from Red database and put into black database. If nodes are not has better performance than timestamp will be zero after maximum. Statistics are usually upon the node behaviors. In this IDS statistics of particular node are made by its neighbors. It consist of following

If statistic goes lower than particular nodes have to improve in performance if it goes higher than it mention as bad node. The ith is a time which show that calculation had made at ith time. The ith time interval is not fixe between nodes or routers. Threshold is boundary between normal and bad nodes/routers in this Red database and it is fixe in all entire networks.

Front level deals same like above mention work at individual nodes which are inter-connect each of them. When intrusion node is founds than information flood in whole network. The broadcasting node also report to mesh router to initiate the backbone level. When more than one same report are receive than mesh router send the information to other mesh routers as well as gateway routers. Same process run again at router level, these routers independently investigate like neighbors nodes investigate. If it sure than particular node put in Red DB and flood only latest information in entire network whereas share whole database to other mesh router like Front level node working.

3.2.2. BLACK Database:

Black DB consist of those nodes/ routers which are new entry position in entire network or have bad reputation about its behaviors in any case like packet dropping or involve to generate intrusion. In this database, node and router make entries individually at its standing position in entire network.

When new node are found/ introduce by hello packet with other nodes or routers ,its entry put in black database and make its statistic zero at ith time. Send different type of data packets throw this new node to judge it performance by its neighbors. Whenever statistic make like in fig3.6, the chunks of latest information broadcast to its neighbors. So every request from any new individual is monitor and use to make behaviors in positive or negative sense. The black

database have threshold to define boundaries of normal nodes/ routers behaviors. If statistics which are calculated by its neighbors to show its performance is lower than threshold which are fixe through all network are black database else it remove from this database and list in RED database. If black database is an update at ith time about particular nodes performance than broadcast latest chunks to its neighbors. If updated neighbor's chunk receive about particular node than update black database.

Black database table

NODs	Status	Ith Time	100> Statistics < threshold 500
node 2	Active	02:14:11	402
node 8	Busy	02:15:17	null
node 15	Off	Last 01:57:48	300
node 1	Intrusion	Null	null

Fig 3.6

In fig 3.6, threshold is 500 where bottom limit is 100. If any node performance which update by ith time is less than bottom limits it remove from black database and list in Green database. Status Active mean, node is free to communicate or have no queue of data packets or can listen your request frequently. Status busy mean, node is busy in processing queues of requests from other mesh nodes, show by its statistics is null, not goes updated at ith time interval. The advantage of this entry is that neighbor node scan understands and makes other path for forwarding their data packets. Status off mean, node is invisible or off or power failure node but have normal statistics at last ith time. That node will remain in black database until not goes on. Only latest ith entries which node make individually, will share with neighbors so that network not going to busy. Whenever latest entry come about any node from its neighbors than flash pervious entry or update with new entry but not share.

Intrusion generator nodes are listing in Black database when there are newly introduce. Treat them same like other to build their statistics. In fig 3.6, their statistics and ith time are representing as null because of their behaviors. Mostly intrusion generator nodes only make a request to other rather than listening request from other. That's way both entries in table represent null. Node checks itself their signature of all well-known intrusion type nodes store in built in database like [12] as independently and cross layer feature sets [12]. If it match than node broadcast to its neighbors and report to network mesh routers as action. When neighbor receive its request for investigate than neighbor make path to that particular node and start to communicate if particular node again try to access privacy of neighbors than neighbors confirm that it is an intrusion node and replay back to that node which requested to investigate and broadcast to its own neighbors. Now confirmations make an entry in RED database and remove from black database. If it is not confirm by neighbors than its entry will remain in black database and check its behavior again.

Front level and backbone level have same procedure which describe above in building black database as individually at node or as router and share with neighbors as cooperatively approach to make better decision to route data packets in WMN.

3.3.3. GREEN Database:

Green database have those types of nodes which are trustful or have good statistics or individual node assign as good node/ router. Trustful nodes are those nodes which are using as common path between nodes. These nodes assign as trust-full status of that particular node in green database at individual. Good statistics have those nodes which have statistics less than bottom level. This type of node measured cooperatively by its neighbors. Good nodes are those which have good

Green database table

NODs	Status	Ith Time	Statistics < bottom level 100
node 12	Trustful	03:14:11	92
node 4	Live	03:15:17	75
node 7	Good	1:57:14	null

Fig 3.8

statistic but no going to update at ith time because of power failure.

When a node mark as trustful node, made by cooperatively communication between its neighbors than flood this information between nodes/ routers. Trustful criteria are that node should be directly connected of those particular nodes/ neighbors. These neighbors make a communication throw that node. When a new node is introduce by hello packets, its neighbors establish a path with that and forward some data packet throw that to monitor its statistics if statistics is not good than encourage to improve its statistic throw different type of packets. When this node improve its statistics and put in that green database than neighbor node watch its statistics and compare with other of own neighbors, if its statistics is lower than all other neighbors assign as trustful node. This update chunk information is flooding in entire network. Mesh routers also receive that information and put that in its green database. When updated chunk of green database is receive at any node/routers than update directly of its own green database. Trustful node is use to make path for better and trustful communication between all nodes.

node always forward data packets throw those nodes which have low statistics. In fig3.8, node12 have lower statistic but status as a trustful node are use as backbone path between nodes or secondary option for forwarding data packets. So nodes always make a path according to its green database. Lower statistics node is select as primary communication source.

When a node is put from black database to green database due to its statistics, just broadcast that type of information between all of its neighbor's, not whole network or mesh routers. When node is invisible or drop lot of data packets or break communication connection with other nodes than its neighbor find out its behaviors. If node is visible and drop lot of data packets than neighbors motivate throw data packets to improve its performance like [8]. But if it continually doing same, its statistic is auto increase and across the bottom limits. It removes from green database and put in to black database. If it is a trustful node than flood this update to all nodes/ mesh routers else only broadcast to its neighbors. A node which has to break directly connection with its neighbors or invisible than its neighbors put its statistic value to null, stop forwarding data packets to that node and continuously monitor by other type of packets to make a connection again. This node remains in green database until it is not again alive. When it is visible than its statistics again measure.

Green database make as individually at standing position of node like black database. Flooding those update chunks of that which are about trustful status nodes. And only other chunks are broadcasting with neighbors which are about performance. And other type of information is not share with any other. Node makes a path before analyze green database statistics. Motivation packets are use to motivate the node about its performance. Green database always partially share not as whole like RED database. Not any node directly shifts from Green database to RED database or vice versa.

4. Discussion:

There are some key points which are important or highly desirable for WMN due to its topology and access points.

1. The proposed RGB IDS must work both as standalone in front level and cooperatively as backbone level in any exiting WMN topology. Both level of propose IDS must work combine as individually at node (end use) and cooperatively at mesh router which are important component of WMN. RED database must be share between nodes/routers and mesh router/access points/ gateway routers.
2. The proposed IDS must handle multilayer security attacks, such as physical layer attacks like jamming, scrambling MAC layer attacks like spoofing, de-authentications etc, network layer attacks like gray hole, false hole etc and transport layer attacks like syn flood. It must use built-in database to match define signatures of its type of attacks and take particular action against them but all are classified as intrusion.
3. These IDS must have to work individually and cooperatively sharing mechanism in any case of intrusion detection. Every new or silence node are also monitored. In any type of environment, it must detect low type of intrusion and responses appropriate define action in cooperatively manner.

5. Conclusion:

Cooperatively approach makes better prevention techniques from intrusion in WMN for secure communication. However in public or commercial sectors, large scale multi-hop WMN in any type of environment faces many security attacks due to older design IDS negligence. These IDS mostly design for Ad-hoc type scenario or those which designs for WMN are limited no of cooperatively communication between nodes/ routers. These are not design for large scale or cannot communicate at individual level to cooperative level which are really need in WMN. We proposed RGB IDS especially for WMN, works in large scale multi-hop at individually and cooperatively level rules. Nodes individually monitor its neighbors, new enter nodes and silence nodes. Make RGB databases, share with neighbors. If an intrusion node are found than report to network router. Broadcast to all, stop communication with that node and block it as individually. Action at individually are also taken, whereas other IDS cannot have that type of features. Mesh routers investigate on more than two same reports from different nodes about that particular intrusion node. Backbone/ cooperatively approach start, everyone can investigate if this node behavior signature match in built-in database or access privacy than action is taken against as cooperatively. Block it entire network. So collectively monitor phase makes common RED database which is flooding entire network by mesh router. Other two databases only share latest chunks with neighbors, not whole databases, for prevention the network from latency. Statistics are made by every neighbor nodes at individually to make perfect path for routing data packets and find multilayer security attacks. Such cooperatively and individually cross layer IDS are design for large scale multi-hop broadband wireless mesh network using IEEE 802.11. Our future work to classify Built-in database and makes different Action according to different type of intrusions found at any type of layer. And cooperatively share information in RED database according to that classification.

6. Acknowledgement:

In writing this Research Paper, I have been fortunate to be assisted by my teacher in many of the sub disciplines that make up the field of Wireless Networks. This Paper

could not have been written without their help. I am deeply indebted to the following, who took the time to review my Paper Drafts and, in many cases, to tutor me and help organize My Research Paper in their individual areas of expertise.

Dr. Fareeha Zafar (Department of Computer Science, GC University Lahore, Pakistan)

I am also grateful to my Co-Author who helped me in various drafts of this Research Paper and who contributed his suggestions.

I would especially like to thank Dr.Fareeha Zafar, who throughout this project was a constant source of encouragement, technical expertise, and support of all kinds.

Reference:

[1] S. McClure, J. Scambray, G. Kurtz (2001),"Hacking Exposed," 3rd ed., McGraw-Hill.

[2] Caballero J (2006), "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks: The Routing Problem," in Proceedings of TKK T-110.5290 Seminar on Network Security, Japan, pp. 1-2.

[3] Shrobe H, Knight T, Hon A (2007), "TIARA: Trust Management Intrusion Tolerance Accountability and Reconstitution Architecture," Computer Science and Artificial Intelligence Laboratory Technical Report, 2007.

[4] Rocke J, Demara F (2006), "CONFIDANT: Collaborative Object Notification Framework for Insider Defense using Autonomous Network Transactions," Computer Journal of Elsevier, Autonomous Agents and Multi-Agent Systems, vol. 12, no. 1, pp. 187-202.

[5] Tseng Y, Balasubramanyam P, Ko C.,Limprasittiporn R, Rowe J, and Levitt K (2003), "A specification-Based Intrusion Detection System for AODV," in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, NY, pp. 1987-1997.

[6] G. Vigna, et al (2004),"An intrusion detection tool for AODV-based ad hoc wireless networks," Annual Computer Security Applications Conf. (ACSAC 2004), Tucson, pp. 16-27.

[7] K. Ilgun, R. Kemmerer, P. Porras (1995),"State transition analysis: a rule-based intrusion detection approach," IEEE Trans. on Software Engineering, vol. 21, pp. 181-199.

[8] Chen M., Kuo S., Li P, Zhu M, "Intrusion Detection in Wireless Mesh Networks", CRC Press, 2007.

[9] H. Yang, J. Shu, X. Meng, S. Lu (Feb. 2006),"SCAN: self-organized network-layer security in mobile ad hoc networks," IEEE J. on Sel. Areas in Communications, vol. 24, , pp. 261-273.

[10] Puttini .S , Percher .M, j, Abbas ,L (2003), "A Modular Architecture for Distributed IDS in MANET," in Proceedings of the International Conference on Computational Services and its applications, Canada, pp. 8-21.

[11] Djenouri D, Khelladi L, Badache N, "A Survey of Security Issues in Mobile Ad-hoc and Sensor Networks," Computer Journal of IEEE Communications Surveys and Tutorials, vol. 7, no.

[12] Shafiullah Khan, Kok-Keong Loo1, Zia Ud Din (Aug 3, 2009) "Framework for Intrusion Detection in IEEE 802.11: Wireless Mesh Networks".

[13] Kargl F, Klenk A, Schlott S, Weber M (2004), "Advanced Detection of Selfish or Malicious nodes: Ad Hoc Networks" CA, pp. 353-362.

Muhammad Salman Ashraf is M.Phil. / MS Computer Sciences with Specialization in Computer Networks in the Department of Information Technology at the University of Central Punjab, Lahore, Pakistan. His Research interests include Network Security, Cryptography and Network Programing.

Muhammad Raheel is M.Phil. / MS Computer Sciences with Specialization in Computer Networks in the Department of Information Technology at the University of Central Punjab, Lahore, Pakistan. He has 4-5 Years of Research and Professional Practical experience. His Research interests include Designing and Configuration of Computer Networks, Network Security and Wireless Networks.