IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, January 2024

# Analysis of a Fuzzy Based Intrusion Detection System in Wireless Ad Hoc Networks

**Tarun Kumar Gaur[1], Ashish Gupta[2], Anuradha Pathak[3]**
Research Scholar, Department of Electronics & Communication[1]
Assistant Professor, Department of Electronics & Communication[2,3]
Nagaji Institution of Technology and Management, Gwalior, India

**Abstract:** Technology and its growth is considerably enormous. This massive growth allows the opening of new fields of application in the domain of wireless networking and mobile ad-hoc networks (MANET) is one of its kinds. Mobile ad hoc network is widely used from collaborative computing to time critical applications in indoor and outdoor environment. Mobility of ad hoc network makes very attractive in all areas of mobile applications. Nodes participating in mobile ad hoc networks are autonomous, self-configurable and act as a router as well. These types of networks are dynamic in nature and have sort life time. Dynamic nature and limitations of the wireless transmission medium make MANET unsecured and vulnerable to various attacks. It is very tough to implement security for this networks and it opens up doors for further research work on this area. There is a great scope for designing a system to identify attacks and take countermeasures to minimize it and keep the performance of the network within acceptable limits. Intrusion detection system is one of its kinds and considered as security mechanism for MANET. This thesis explores different types of intrusion detection system like misuse detection and anomaly detection for mobile ad hoc networks. Anomaly detection techniques for ad hoc networks depend on the characterization of normal behavior pattern of wireless nodes. This research work focuses on wireless node behavior based detection technique. Most of anomaly intrusion detection systems are focusing on upper layer traffic to a profile normal behavior of wireless node. This research work focus on media access control (MAC) layer and network layer of wireless node. It is inefficient to use a large feature set of MAC layer and network layer due to energy limitation in ad-hoc network. A minimal feature set from MAC layer and network layer were proposed. This research work proposed an anomaly intrusion detection system for mobile ad hoc network using fuzzy logic and weighted average method. The network performance of mobile ad hoc network with intrusion detection system was analyzed using various network parameters. Further the performance of the performance of the intrusion detection system was analyzed using detection rate and false alarms. Results show good improvement in detection rate and other performance metrics.

**Keywords:** wireless network , MAC Layer, mobility.

## I. INTRODUCTION

An intrusion detection system aims at finding any anomaly activity in thenetwork. The difficulty in computational overhead to detect intrusive attempt is the main challenge for any IDS. All intrusion detection system has common issues like accuracy, speed and adaptability. An intrusion detection system has to monitor entire network and need to capture large amount of data, further these data are computed to find out potential attack which may degrade the performance of network system in terms of speed and accuracy. A method called weighted average method is proposed in this research which aims at resolving above said issues. This method uses minimal number of parameters to reduce the complexity in computation.

## II. RELATED WORK

Mobile ad hoc networks are divided into two types which are infrastructure network and ad hoc networks. Infrastructure networks use gateways to connect them with other networks (or internet) which are fixed one. Nodes are free to move around and establish a connection with base station which is very close to its range. A node lost a connection with its

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, January 2024

current base station and look for other base station on its range to establish a connection to ensure seamless communication. Other type of network is ad hoc networks which has no infrastructure and don't need routers to establish a communication. All participating nodes will act as routers and a simple node as well. These networks have limited transmission range which forces for the need of multiple hopes. Every node has routing details since all nodes will act as a router, in this way these networks are dynamic in nature and changes its topology very often.

An event that is attempted to compromise the integrity, confidentiality and availability of a resource is called as intrusion. Lot of research works have been conducted on computer network security in last four decades and lot of intrusion detection system (IDS) prototypes has been developed and published. Way back in 1980 one researcher called J.Anderson started a research in this area and published an article [1]. After this lot of prototypes and proposals have been developed and published. Many of them have been documented by an author called Michael Sobirey[2]. An IDS monitors network traffic and looks for suspicious activity, then it alerts the system or network administrator when it detects any suspicious activity. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network

M. Medadian [18] discussed about traffic analysis and location finding.Tracing algorithm were developed and tested with the help of simulation tools. This system was evaluated and discussing about passive routing attacks. Authors developed a routing protocol for passive attacks.

W. Scheirer [22] discussed an effective technique to detect denial of service attack and proposed a solution to this attack. The availability of node is checked with help of various parameters used i.e. battery power, RTT, total time taken by packets,total number of packets forwarded, blacklist used for attackers. The attacker is detected by setting different threshold values for each category. These threshold values are compared with number of packets delivered, further nodes are checked forthe status of blacklist. But this detection technique was specific to AODV and DSR protocols in MANET. Marti et al [23] proposed a mechanism to mitigate the effect of packet dropping, which has two mechanisms called watchdog and pathrater. This mechanism mitigates number of misbehaving nodes in MANET. G. Xiaopeng [24] proposed a method to detect suspicious node, this technique identifies the node that drops packets using global trust value of neighbor nodes. This method showed an improvement in terms of low false alarm rates and compared with watchdog algorithm [23].Black Hole Attack. Blackhole attack is one type of denial-of-service attack in which a router drops packets instead of forwarding it. This will happen if the router becomes compromised node for various reasons. Emma Ireland [23] described in detail about black hole attack in AODV protocol network. A node sends RREQ if it wants to know the route to the destination. An intruder broadcasts itself as having fresh route and sends reply to this RREQ to become a member of that route. By repeating this to more RREQ's this intruder becomes a intermediate node and starts dropping packets instead of forwarding it. In this way, the intruder becomes part of the route to destination.

Jing Nie [24] summarized the survey of existing routing protocol used in wireless mobile ad hoc networks. Togbad [40] describes a black hole detection mechanism, which uses topology graph to detect attacks. This method was developed for the OLSR proactive routing protocol, however it would not be effective for reactive routing protocols because of acquiring entire topology information is not feasible. DharaBuch [36] proposed a black hole detection method for AODV. The concept in this technique is that on receiving a reply, the receiver node initiates a judgment process about the replier. A neighbor shares their opinion about the replier. A decision is made based on number (a fixed threshold) of packets, if a node receives many packets but does not forward certain number of packets then it is considered to be malicious.

Above intrusion detection systems work with specific attack based detection methods and not able to detect more attacks [14]. Anomaly intrusion detection works efficiently for detection of all kind of attacks. Anomaly detection techniques for ad hoc networks depend on the characterization of normal behavior pattern of wireless nodes. This research work focuses on wireless node behavior based detection technique. Most of the anomaly intrusion detection systems are focusing on upper layers traffic to profile normal behavior of wireless node. This research work focus on only MAC and network layer of wireless nodes. It is inefficient to use a large feature set of MAC layer and network layer due to energy limitation in ad-hoc network.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, January 2024

## III. METHODOLOGY

### 3.1 PARAMETERS DEFINED IN WEIGHTED AVERAGE METHOD

This thesis uses five parameters to compute the weight value to identify malicious activity for mobile ad hoc network. The parameters defined are given below.

- Channel Utilization Ratio (CUR)
- Successful Connection Ratio (SCR)
- CTS Received Rate (CTS_RR)
- Successful Data Forward (SDF)
- RTS Retransmission Count (RTS_ReC)

Channel Utilization Ratio (CUR) : Channel Utilization Ratio is a ratio between neighbors channel utilization time and node level channel utilization time.This value is computed for each node and stored in neighbor table. Channel utilization time is calculated using network allocation vector (NAV). Wireless network protocol of ad hoc network uses virtual carrier-sensing mechanism called NAV. This virtual carrier sensing is a technique that handles the nodes access to the physical medium. Logically NAV is a counter, which goes down to zero at frequent time interval. The counter value zero is an indication that the medium is idle and counter value other than zero indicates that the medium is in busy state.

Successful Connection Ratio (SCR): Wireless network uses a handshaking technique to establish a connection using MAC layer feature set called Ready To Send (RTS) and Clear To Send (CTS). A destination node sends CTS to the source node for every RTS it receives. Successful Connection Ratio is a ratio between CTS received and RTS send.

### 3.2 DETECTION ALGORITHM

This section of the thesis details about how parameter values are calculated and how combined weight value (CTw) is computed. The definitions of parameters aregiven in previous section. Now the procedure to calculate parameter values is given below.

- Check Neighbours Channel utilization time using NAV (Nb_CU)
- Find NAV – Busy state for each node.
- Apply Listen method to find the channel utilization
- Find Node level Channel utilization for each node (Node_CU)
- Channel utilization time for own transfer of every node.
- Compute Utilization ratio (CUR)
- Channel Utilization Ratio (CUR) = Node_CU /Nb_CU
- In MAC each node send RTS and CTS.
- Successful Connection ratio (SCR) = CTS Received / RTS sent
- CTS Received Rate (CTS_RR):
- CTS broadcast to one hop nodes.
- Compute CTS received Count for every node.
- CTS_RR = number of CTS packet received per second
- Compute Successful Data Forward (SDF) Count for Data PKTS.
- SDF = Number of data PKT Forward / Number of data pkt received.
- Check RTS Retransmission count (RTS_ReC)
- RTS_ReC = Number of RTS packet retransmitted.
- Update NBR table with following data
- Node id.
- Channel Utilization Ratio (CUR).
- Successful Connection ratio. (SCR)
- CTS_RECV_RATE (CTS_RR)
- Successful Data Forward count (SDF)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, January 2024

- RTS_ReC

A table called neighbor table (NBR table) is created to store parameter values which are calculated using above procedure. Now weighted average method is introduced to compute Combined Weight (CTw).

### 3.3 WEIGHTED AVERAGE INTRUSION DETECTION SYSTEM (WIDS)

Weighted average is a logical abstraction in which a weight is assigned to each parameter to be averaged. These weightings determine the relative importance of the parameter on the average. An equal weight value is assigned for like items, which means that parameters with equal importance may have same weight value. The procedure to compute weight value is given below.

Calculate total weight of parameter one (T1) by multiplying W1 and CUR.
Find CUR value from NBR table.
Assign weight value W1 to CUR.
T1-W1*CUR
Calculate total weight of parameter two (T2) by multiplying W2 and SCR.
Find SCR value from NBR table.
Assign weight value W2 to SCR.
T2-W2*SCR
Calculate total weight of parameter three (T3) by multiplying W3 andCTS_RR.
Find CTS_RR value from NBR table.
Assign weight value W3 to CTS_RR.
T3-W3* CTS_RR
Calculate total weight of parameter four (T4) by multiplying W4 and SDF.
Find SDF value from NBR table.
Assign weight value W4 to SDF.
T4-W4* SDF
Calculate total weight of parameter five (T5) by multiplying W5 and RTS_ReC.
Find RTS_ReC value from NBR table.
Assign weight value W5 to RTS_ReC.
T5-W5* RTS_ReC

The parameter values stored in NBR table is moved to another table called periodic table. This table is used to calculate total weight value. Initially each defined parameter is assigned a weight say W1 is assigned to CUR, W2 is assigned to SCR,W3 is assigned to CTS_RR, W4 is assigned to SDF and W5 is assigned to RTS_ReC.These weight values is multiplied with parameter value and stored as T1, T2, T3, T4and T5 respectively. After this all these values are added together to calculate the Combined Weight (CTw) value.

$$\mathbf{CTw = T1 + T2 + T3 + T4 + T5}$$

The sum of all weight values is equal to 1. Combined Total Weight CTw varies with respect to the communication activity of the nodes. Fixing up the threshold is major problem for anomaly detection in intrusion detection system. Priority is given to this problem and solved very carefully in weighted average method. The threshold value was fixed by analyzing the output of various scenarios and extensive research work. A node which exceeds this threshold value is identified as a malicious node. That malicious node is excluded from the network topology by adding node id into blacklist.

## IV. RESULT AND DISCUSSION

Network simulator 2 (NS2) is used for the simulation model. The NS-2 parameters are listed in Table-1. 600mX600m field with 100 nodes are deployed using random waypoint mobility model. Continuous Bit Rate (CBR) application traffic is used for the coverage area of 100m.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, January 2024

**Table – 1 Simulation Parameters**

| PARAMETER VALUE | PARAMETER VALUE |
|---|---|
| Topology | 600m X 600m |
| Node movement | Random waypoint model |
| Speed | 0-10m/s |
| Wireless node count | 150 |
| Total number of flows | 25 |
| Average transmission rate per flow | flow 2 packets/s , 512b/packet |
| Send buffer at each node a fixed | A fixed 64-packet |
| Testing Execution Time | 200s |

The NS2 instructions are used to define the topology structure of the network and the motion of the nodes. Each packet starts from a random source to random destination with a randomly chosen speed. A pause time of 0 second corresponds to the continuous motion of the node and a pause time of 200 seconds corresponds to the time that node is stationary and following scenario is assumed.

### 4.1 SCENARIOS

Various scenarios are simulated in this model and some them are listed below for better understanding about scenarios created in simulation environment.

- Scenario Without Attack
- Take the output for single traffic.
- Take the output for Dual traffic

o Select two traffic without interfering with each other (source, destination or forward node)
o Select two traffic with interfering with each other

- One destination interfere with other traffic source node
- One destination interfere with other traffic Destination node
- One destination interfere with other traffic forward node
- One source node interfere with other traffic source node
- One source node interfere with other traffic Destination node
- One source interfere with other traffic forward node
- Take the output for Multiple Traffic

**Scenario With Attack**

Take the output for single traffic with one attacker

- One attacker node interfere with other traffic source node
- One attacker node interfere with other traffic Destination node
- One attacker node interfere with other traffic forward node

Take the output for single traffic with Multiple attacker. Figure 1 and figure 2 shows the screen shots of the transmition scenarios. Figure 1 shows a scenario without attacker nodes and this transmission scenario was created with 150 mobile nodes

Figure 2 is a screen shot of a mobile ad hoc network environment simulated using 150 mobile node with a topology range of 600m * 600m. Wireless nodes with green color are normal nodes and blue color nodes are attacker nodes in this transmission scenario.

In the experimental study, the weighted average value is computed to fix a threshold level. Initially the feature set values stored in neighbor table are fetched and calculated corresponding parameter values, further these parameter values are stored in periodic table to compute individual parameter weight value and combined weight value. Period table contains the details of current node id, neighbor node id, time stamp and parameter values with corresponding weight values.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, January 2024

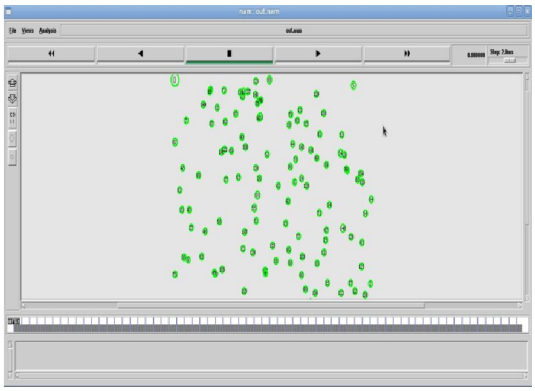

Figure 1 Ad hoc network with 150 nodes

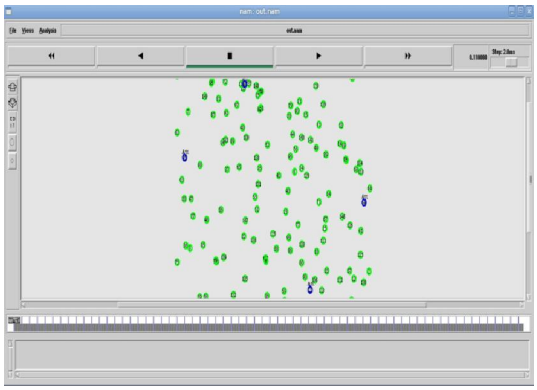

Figure 2 Ad Hoc Network with Attacker Node

These feature set values are picked to calculate the parameter values defined, further these parameter values are used to compute weighted average value. Each individual parameter value is multiplied by its corresponding weight to arrive individual parameter weight value. Then all these individual parameter weight values are added together to calculate combined weight value. This combined weight values is compared against the threshold value to detect intrusion.

Performance parameters like false alarms and detection rates of anomaly intrusion detection were analyzed. Following assumptions are considered in weighted average method.

Feature set value collection mechanism should not compromised at any time during system operation.

It is assumed that there should not any attack for during initial time say 20 or 25 seconds.

Table-2 is a replica of the periodic table used in weighted average method. Table 2 contains above said values for current node id 59 and neighbor node ids of 91, 92, 1nd 93. In this scenario the actual attack is mounted at 30th second and attack end time is 80th second. The period table values are updated for every 5 seconds.

Table 2 Data stored in Neighbour (NB) Table

| CurNode | NB Node | Time | $CT_w$ | W1 | CUR | T1 | W2 | SCR | T2 | W3 | CTSRR | T3 | W4 | SDF | T4 | W5 | RTS Rtx | T5 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 59 | 91 | 55 | 0.276 | 0.3 | 0.055 | 0.017 | 0.2 | 1 | 0.2 | 0.3 | 0.2 | 0.06 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 91 | 60 | 0.276 | 0.3 | 0.055 | 0.017 | 0.2 | 1 | 0.2 | 0.3 | 0.2 | 0.06 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 91 | 65 | 0.276 | 0.3 | 0.055 | 0.017 | 0.2 | 1 | 0.2 | 0.3 | 0.2 | 0.06 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 91 | 70 | 0.276 | 0.3 | 0.055 | 0.017 | 0.2 | 1 | 0.2 | 0.3 | 0.2 | 0.06 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 91 | 75 | 0.276 | 0.3 | 0.055 | 0.017 | 0.2 | 1 | 0.2 | 0.3 | 0.2 | 0.06 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 91 | 80 | 0.276 | 0.3 | 0.055 | 0.017 | 0.2 | 1 | 0.2 | 0.3 | 0.2 | 0.06 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 91 | 85 | 0.276 | 0.3 | 0.055 | 0.017 | 0.2 | 1 | 0.2 | 0.3 | 0.2 | 0.06 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 91 | 90 | 0.276 | 0.3 | 0.055 | 0.017 | 0.2 | 1 | 0.2 | 0.3 | 0.2 | 0.06 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 92 | 20 | 0 | 0.3 | 0 | 0 | 0.2 | 0 | 0 | 0.3 | 0 | 0 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 92 | 25 | 0 | 0.3 | 0 | 0 | 0.2 | 0 | 0 | 0.3 | 0 | 0 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 92 | 30 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 92 | 35 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 92 | 40 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, January 2024

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 59 | 92 | 45 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 92 | 50 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 92 | 55 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 92 | 60 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 92 | 65 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 92 | 70 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 92 | 75 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 92 | 80 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 92 | 85 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 92 | 90 | 0.433 | 0.3 | 0.051 | 0.015 | 0.2 | 0.79 | 0.16 | 0.3 | 0.8 | 0.24 | 0.1 | 0.1 | 0.01 | 0.1 | 0.2 | 0.01 |
| 59 | 93 | 20 | 0 | 0.3 | 0 | 0 | 0.2 | 0 | 0 | 0.3 | 0 | 0 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 93 | 25 | 0 | 0.3 | 0 | 0 | 0.2 | 0 | 0 | 0.3 | 0 | 0 | 0.1 | 0 | 0 | 0.1 | 0 | 0 |
| 59 | 93 | 30 | 0.188 | 0.3 | 0.028 | 0.009 | 0.2 | 0.55 | 0.11 | 0.3 | 0.2 | 0.06 | 0.1 | 0 | 0 | 0.1 | 0.2 | 0.01 |

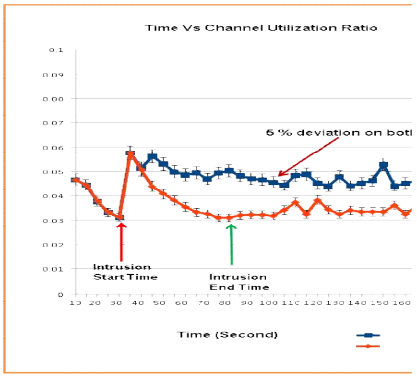


Figure 3 Time Vs Channel Utilization Ratio

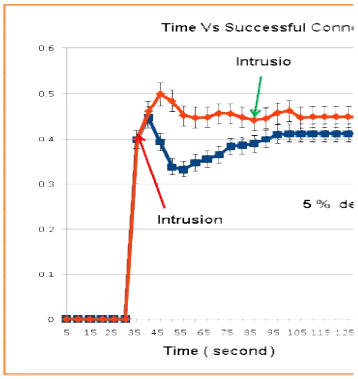


Figure 4 Time Vs Successful Connection Ratio

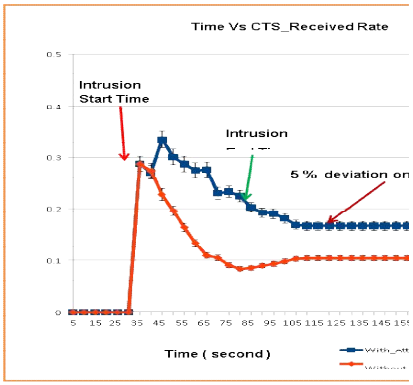


Figure 5 Time Vs CTS Received Rate

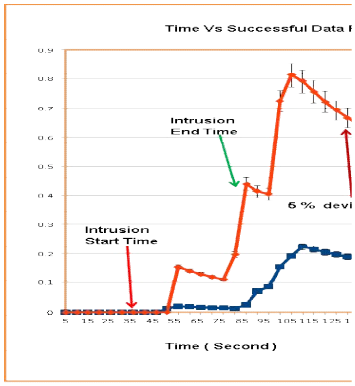


Figure 6 Time Vs Successful Data Forward

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, January 2024

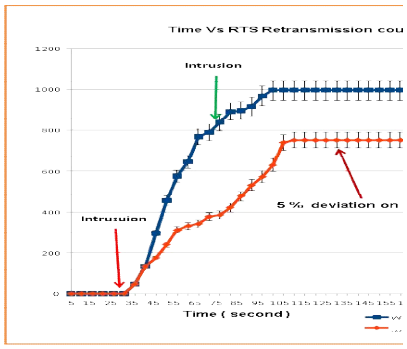


Figure 7 Time Vs Successful Data Forward

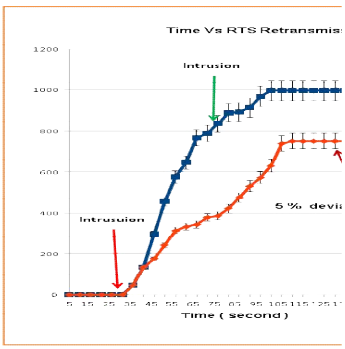


Figure 8 Time Vs RTS Retransmission Rate

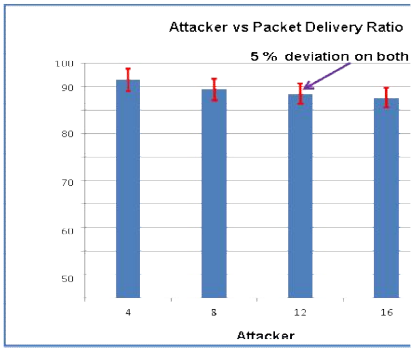


Fig 9 Attackers Vs packet delivery ratio for WIDS

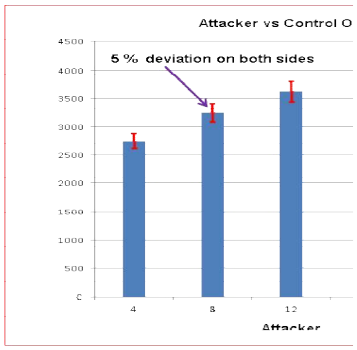


Figure 10 Attackers Vs Network Control Overhead for WIDS

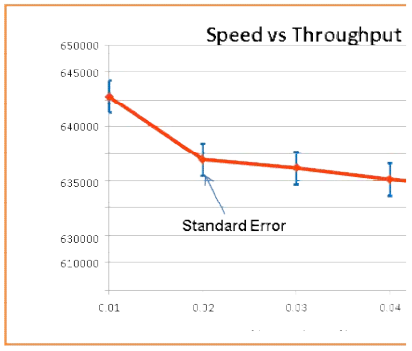


Figure 11 Throughput Vs Node speed for WIDS

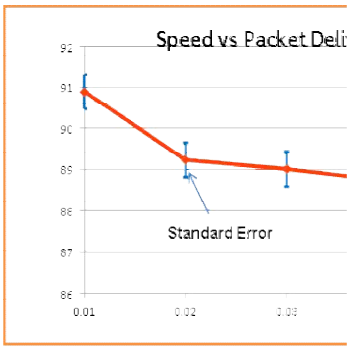


Figure 12 Packet Delivery Ratio Vs Node speed for WIDS

## V. CONCLUSION

Various financial possibilities which are opening up through wireless network have made intrusion detection a crucial issue in wireless computing systems. This research work addressed security problems in wireless ad hoc networks. The main goal of anomaly intrusion detection system is to minimize the false alarm rate and to improve the detection rate. Misuse intrusion detection is inadequate to detect all types of intrusion due to the advent of new attacks and system vulnerabilities that necessitate the development of anomaly detection based IDS.

## REFERENCES

[1] J. Anderson., 1980, "Computer Security, Threat monitoring and surveillance",Fort Washington PA, James P, Anderson & Co.

[2] Michael Sobirey, "Intrusion Detection Systems Bibliography", available athttp://www.cse.sc.edu/research/isl/mirrorSobireys.shtml pp. 351-367.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, January 2024

[3] N.Ye, X.Li, Q.Chen, M.Emran and M.Xu., July 2011, "Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data", IEEE Transactions on Systems, Man, and, Cybernetics, Vol. 31, No. 4
[4] N.Ye and Q.Chen, 2012, "An Anomaly Detection Technique based on a CHISQUARE Statistics for Detecting Intrusion into Information System", International Journal of Quality and Reliability Engineering International, Vol.17, No.6, pp 105-112..
[5] H. Debar, M. Becker and D. Siboni, May 1992, "A Neural Network Component for an Intrusion Detection System", Proceedings,. IEEE Computer Society Symposium on Security and Privacy, Oakland.
[6] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, Oct 2007, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," IEEE Wireless Communications Magazine,Vol.14, No.5, pp. 56-63.
[7] D. Kheyri and M. Karami, 2012, "A comprehensive survey of anomaly based intrusion detection systems in MANETs", Journal of Computer and Information Science,Vol.5,No.4, pp.132-139.
[8] S. Sahu and K. Shandilya, 2010, "A Comprehensive Survey on Intrusion Detection in MANET", International Journal of Information Technology and Knowledge Management, Vol.2, No. 2, pp. 305-310.
[9] J.C. Kao and R. Marculescu, 2006, "Eavesdropping Minimization via Transmission Power Control in Ad Hoc Wireless Networks", Proceedings,.IEEE Sensors and Ad hoc Communication and Networks SECON.
[10] T. He, H. Wang and K.W. Lee., Nov 2008 "Traffic analysis in anonyms MANETs",Proceedings,. IEEE Military Communication Conference MILCOM.
[11] J. Kong, X. Hong and M. Gerla., Oct 2008, "A new set of passive routing attacks in Mobile ad hoc networks", Proceedings,. IEEE Military Communication Conference MILCOM.
[12] Neha Singh SumitChaudharyKapil Kumar Verma A. K. Vatsa., Sep 2012," Explicit Query based Detection and Prevention Techniques for DDOS in MANET". International Journal ofComputer Applications (0975 – 8887) Volume 53– No.2.
[13] S. Marti, T.J. Giuli, K.Lai and M. Baker., 2000, "Mitigating Routing Misbehaviou1r in Mobile Ad Hoc Networks", Proceedings, International Conference on Mobile Computing and Networking, pp 255- 265.
[14] J. Sen, M. Chandra, P. Balamurlidhar, S.G. Harihara and H.Reddy., 2007, "A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad hoc Networks", Proceedings, IEEE (ICT-MICC).
[15] S. Kurosawa and A. Jamalipour., Nov 2007, "Detecting Blackhole Attack on AODV based Mobile Ad Hoc Networks by Dynamic Learning method", International Journal of Network Security, Vol.5, No.3, pp 338-345.
[16] F.Tseng, L. Chou and H.Chao., 2011, "A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks", Journal on Human-Centric Computing and Information Sciences, Springer, Vol.1, No.4, pp. 1-16.
[17] Y.Hu, A. Perrig and B. Johnson., 2003, "Rushing Attack and Defense in Wireless Ad Hoc Networks Routing Protocol", Proceedings,. ACM Workshop on Wireless Security, pp. 30-40.
[18] M. Medadian, M.H. Yektaie and A.M. Rehmani., Nov 2009, "Combat with Black Hole Attack in AODV Routing Protocol in MANETs", Proceedings,.IEEE Asian Himalayas International Conference on Internet.
[19] AdnanNadeem , Michael P. Howarth., 2014, "An intrusion detection & adaptive response mechanism for MANETs", Ad Hoc Networks 13 (2014) 368–380, Elsevier.
[20] O.F. Gonzalez-Duque, G. Ansa, M. Howarth and G. Pavlou., June 2008, "Detection and Accusation of Packet Forwarding Misbehaviour in Mobile Ad hoc Networks", Journal of Internet Engineering, Vol.2, No.8, pp 181-192.
[21] O.F. Gonzalez-Duque, A.M. Hadjiantonis, G. Pavlou and M. Howarth., June 2009, "Adaptive Misbehaviour Detection and Isolation in Wireless Ad Hoc networks Using Policies", Proceedings, IFIP/IEEE International Symposium on Integrated Network Management (IM 2009), pp 242- 250, NY, USA.
[22] W. Scheirer and M. Chuah., 2008, "Syntax vs. Semantics: Competing Approaches to Dynamic Network Intrusion Detection", International Journal of Security and Networks, Vol. 3, No. 1, pp. 24 – 35.
[23] Emma Ireland, 2013, "Intrusion Detection with Genetic Algorithms and Fuzzy Logic", UMM CSci Senior Seminar Conference, December 2013 Morris, MN.
[24] JingNie* , JiangchuaWen, JiLuo, Xin He, Zheng Zhou, 2006, "An adaptive fuzzy logic based secure routing protocol in mobile ad hoc networks", Fuzzy Sets and Systems 157 (2006) 1704 – 1712 © 2006 Elsevier
[25] E.Padilla, N.Aschenbruck, P.Martini, M.Jahnke and J.Tolle., 2007, "Detecting Black Hole Attack in Tactical MANETs using Topology .Graph", Proceedings,.IEEE Conference on Local Computer Network