An Efficient Algorithm for TCP Attacker Traceback and Countermeasures in MANET using Agents

P.Ramesh
Dept. of Computer Technology,
Anna University, MIT Campus,
Chennai, India

H.Abdul Rauf, Ph.D
Principal,
Dhaanish Ahmed Institute
oftechnology,
Coimbatore, India

P.Mahalakshmi
Dept. of Computer Technology,
Anna University, MIT Campus,
Chennai, India

ABSTRACT
TCP based Denial of Service attacks can cause major problems in Mobile Ad hoc Networks. Tracing the attacker's originand introducing a proper action to retaliate the attacker are the enduring tasks. Surviving methods suffer from major problems due to the typical behavior of Mobile Ad hoc Networks. Then a new bracing methodology is introduced to detect the type of attack and it's origin in MANET using Traffic report. Based on simulations, the attacker origin is tracked down and gives proper countermeasures to retaliate the attack in Mobile Ad hoc Network with low overhead in both communication and computation.

Index Terms
MANET, TCP attacks, Traffic report database, Agent.

1. INTRODUCTION
A Mobile Ad hoc Network consists of wireless mobile nodes as a system that self-organizes dynamically into arbitrary and temporary network topologies. In Mobile Ad hoc Network, nodes can directly within their radio ranges communicate with all other nodes; whereas the nodes that are not in the direct communication range use intermediate node(s) to communicate with each other. Mobility and Multi hop are the main characteristics of Mobile Ad hoc Network. These characteristics make MANET's more vulnerable than the wired networks.

1.1 Attacks in MANET
The Mobile Ad hoc Network mainly poses two kinds of threats. They are internal and external attacks. Internal attacks are those in which the attacker needs to have the normal access to the network activities, by some unauthorized impersonation as a new node in the network, or by compromising a current node in order to conduct misbehaviors in the network. External attacks are those in which the attacker's aim is to cause congestion, propagate fake routing information or making disturbance by providing services. Internal attack also includes traffic flooding, fake authentication and compromised host that sends false information. External attack also includes MAC layer jamming and traffic analysis.

1. SYN Flooding based DoS attacks: This attack misuses the vulnerability of TCP specification. The attacker sends a numerous number of SYN packets which exploits the victim's backlog queue. This causes the entire new incoming SYN requests to be withdrawn by simply dropping it out. [1].
2. Distributed Denial of Service (DDoS) attack: DDoS attack [1] is a type of Denial of Service attack in which a multitude of compromised nodes attack a single target simply in order to waste the resources such as bandwidth, computing power of the victim.
3. Session Hijacking: This attack [10] exploits a valid node's session, in order to receive unauthorized access using a session key to view or modify information and services in the node.
4. TCP ACK Storm: This attack is started only completing a session hijacking attack. If the session is hijacked by a malicious node before, it starts sending ACK packets again and again which will create a storm of TCP ACK[2].

As a result of those attacks discussed above, various anomalies are being created both in the victim nodes and in the network. These anomalies are listed as symptoms (Table 1.1)of the attacks in the network [3][4].

1.2 Proposed Idea
In this paper, a new bracing methodology is being proposed to trace the TCP attacker by detecting the type of attack in the network and to give proper countermeasure for the attacker. To trace back the attacker's origin, TCP traffic report database is widely used. In this method, Static Cognitive Agent (SCA) along with Mobile Cognitive Agent (MCA) [3] is deployed for data collection, attack detection, attacker origin identification, attacker trace back and countermeasure.

Section II clearly demonstrates the existing literature which is related to the proposed work. The proposed work along with algorithmic illustration is defined in Section III. A detailed analysis of results and performance was quoted in section IV. Section V concludes and summarizes the paper along with future support.

2. RELATED WORK
SYN flooding attack causes the network to behave abnormally. The traffic volume changes abnormally during the attack which may result in packet delay, decrease in dropping rate, etc there by increasing the congestion in the network. Shin et al. in their work [5] proposed a method which monitors the SYN Arrival Ratio. Yuichi Ohsita et al. [6] proposed a method which statistically investigates the arrival rate of SYN packet using normal distribution. Satishbabu et al. [7] proposed a novel authentication scheme based on transaction for mobile communication using mobile agents.

To efficiently trace back the DoS/DDoS attacker in a network several algorithms have been developed. Xin Jin et al. [8] proposed Zone Sampling based Attacker Trace back which is an extension of Probabilistic Packet Marking Method [9]. Kim and Helmy used a Small World trace back approach [13] for tracing

the DoS attacker in the network. A further extension to their method CATCH [10] was proposed by Yongjinkim which utilizes MAC and Network layer information Nishanth et al. [11] discovered a novel method which uses Traffic History (MAITH) for TCP attacker Identification.

The existing methods have problems such as increased overhead in terms of memory, CPU and power which is beyond the affordable range of MANET. Our proposed algorithm uses minimal power, CPU and memory and is more robust in untrusted environment and gives proper countermeasures for the attacker.

3. THE PROPOSED ALGORITHM

When an abnormal behaviors detected in the network, then the the super node is informed by the victim node in the network. The super node set up the Mobile Cognitive Agent (MCA) in the victim node which carries the attack detection algorithm. This MCA recognizes the attack type and it's symptoms in order to super node. The super node identifies the attacker zone using the attack history database which is present in it. The MCA is deployed to the particular zone and it starts searching for the abnormal node in that zone.

3.1 The Network Model

The network model for this environment is a super market as shown in the fig. 1. The MANET in the super market is divided into 8 zones.

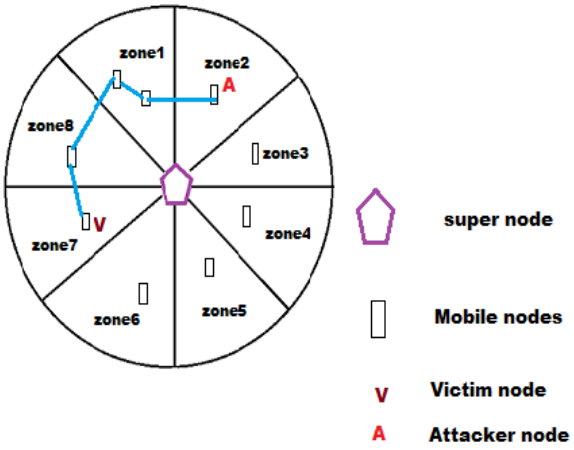

Fig.1 MANET Environment in super market

A super node is chosen to be the node with the good resources in the network. The super node analyses the traffic flow in the network and records and maintains it in the attack history database. A super node contains the attack type, it's symptoms, and it's frequency from a particular zone, in the network.

3.2 System Architecture

The System consists of three modules which also contains the countermeasures placed in the super node. The modules are co-ordinate by the super node. The Data collection module periodically monitors the TCP traffic and forms the attack history database if any abnormality is found in the network.

The Main module enables the Attack Detection module which detects the attack type and it's zone is detected using attack history database. Super node is responsible for all the modules and it has a Static Cognitive Agent (SCA) which initiates the MCA to be deployed to the attacker's zone. The system architecture is illustrated in Fig.2.

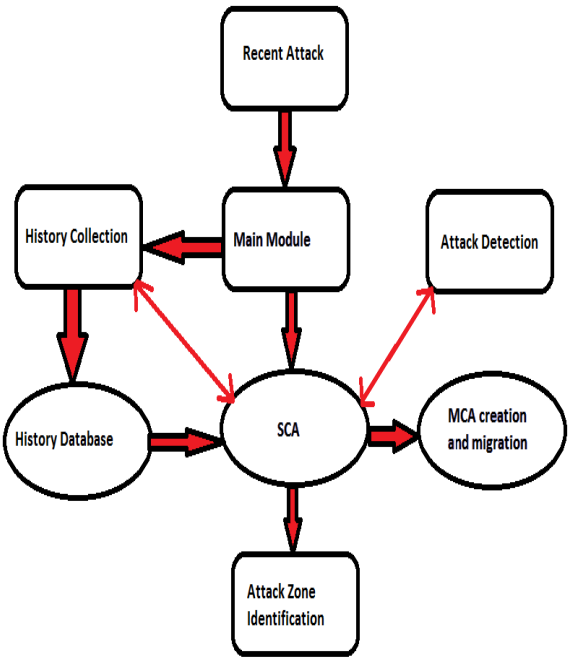

Fig. 2 System Architecture of Agent Model

3.3 Data Collection

A attack history database is being created and stored by the super node as shown in [i.e., TABLE 1] and[i.e., TABLE 2] respectively. TABLE 1contains the symptoms of all attacks that have occurred in the network.[i.e., TABLE 2] contains the type of attack that occurred with the frequency of the attack from the particular zone. [i.e., TABLE 2] is updated with the help of Data collection module initiated by SCA in the super node.

If any node detects any abnormality or symptoms in the network, it informs the super node in the network. The SCA in the super node initiates the detection of the attack by deploying MCA to the particular node. The MCA collects all the symptoms available in the network and informs it to the super node. The SCA in the super node prepares/updates the symptoms table [i.e.,TABLE 1]. After a successful traceback of the attacker the Data Collection module prepares/updates the [i.e., TABLE 1].

Table1: Types of attacks and symptoms

Types of Attack	Symptoms
SYN Flooding Attack	• High packet rate. • Flooding packet's size is 40 bytes. • Number of outgoing packets from Victim is low. • Flooding packets originating from a single source. • CPU utilization of victim is high. • Victim cannot accept new Connections. • Backlog queue of the victim becomes full. • If attacker uses a valid address,then there will be a increase in the number of RST packets in the network. • Increase in number of SYN-ACK retransmission from the victim.
Session Hijacking	• Victim undergoes DOS attack. • Received signal Strength (RSS) will have an abrupt change.
TCP ACK	• High packet rate.

Storm	• Flooding packet's size is 40 bytes. • Number of outgoing packets is equal to number of incoming packets. • High CPU utilization of victim.

3.4 Attack Detection

Distinct algorithms are stored in the attack detection module for SYN Flooding attack detection, TCP ACK storm detection and Session Hijacking. TCP control segments are being extracted from the incoming packets for detecting SYN Flooding attack.

Table2: Attacker History Database

Types of attacks	**No. of times**	**From zone1**	**From zone2**	**From zone3**	**From zone4**	**From zone 5**	**From zone 6**	**From zone 7**	**From zone 8**
SYN flooding attack	31320	45 (0.0014)	15 (0.004)	8 (0.002)	2156 (0.6887)	56 (0.01)	9587 (0.30)	16 (0.05)	24 (0.08)

TCP segments are classified as SYN, RST and FIN based on the flags set in the packet header. SYN Arrival Ratio (SAR) is calculated and SAR is the ratio of incoming SYN segments to the total number of incoming TCP segments. The mean SAR is calculated using exponential weighted moving average (EWMA).By using Adaptive Threshold algorithm [4], an anomaly in mean is identified. TCP ACK storm is detected by monitoring the incoming and outgoing TCP ACK .size if 40 bytes. If it is above a particular threshold it indicates the TCP ACK storm attack. For detection of Session Hijacking, Received Signal Strength (RSS) profile has been calculated by each node for a session between the respective nodes and is updated regularly for each session.

Algorithm for history collection

```
while(1)
{
    if(abnormality)
    {
        Attack_Detection(MCA);
        Update(Symptoms_table);
        Attacker_Traceback(MCA);
        Calculate_Attackzone();
        Update(attack_history);
    }
    else
    {
        break;
    }
}
```

If an attacker does session hijacking, the RSS value changes abruptly which indicates the session hijacking attack.

3.5 Attacker origin Detection

Initially, there will not be any attack history information stored in the history database. Once the attack occurs in the network, the SCA in the super node deploys the MCA in all zones. For each attack that occurs in the network history database is updated. The SCA initially gives importance to the attack history information which is explained in equation 1. As history builds up, more importance is given to the database and attack zone is estimated based on that information.

$$P_s^i(n) = \beta_n * (1 / N) + (1 - \beta_n) * W^i_H(n - 1) \quad (1)$$

Where

$P_s^i(n)$: Probability that SCA in the super node deploys MCA to i^{th} zone.

N : number of zones (i=1 to N)

n: number of times a particular attack occurred in the network

$(1 - \beta_n)$: Weightage given to history information.

β_n:*max* $((\beta_0 - n), 0)$

where $\beta_0 = 1$ and = small increment (here , 0.001)

$W^i_H(n - 1)$: frequency of the attack occurred from i^{th} zone.

$W^i_H(n - 1) = x_i / (n-1)$ where x_i is the number of times a particular attack occurs from i^{th} zone.

3.6 Attacker Trace back

After the identification of attack in the network, the SCA calculates the Psi (n) for each zone in the network. Then, the SCA deploys MCA to the nearest node in the zone having highest Psi (n). MCA checks the behaviour of migrated node as well as neighbouring nodes (by overhearing).

Algorithm for attacker traceback

```
While(1)
{
    Attack_Detection(zone_id, Symptoms_table);
    Pid[]=Compute_probability(zone_id);
    Nearest_node_id = Calculate_nearest(zone_id, Pid[]);
    Send_Agent(zone_id, super_node,Nearest_zone_id);
    LOOP:
    While(nodes!=Bordernodes)
    {
        Node[]=Node_in_Vicinity(zone_id);
        Send_Agent(zone_id, Super_node, Node[i]);
        if(abnormality)
        {
            Send_Agent(zone_id, Node[i], super_node);
            Calculate_TTL(Node[i]);
        }
        else
        {
```

```
        Migrated_id=Behavior_Check(zone_id);
        Send_Agent(Zone_id, Supernode, Migrated_id);
      }
    }
    if(Normal_behaviour(zone_id))
    {
      Zone_id = Calculate_zoneid(pid[i+1]);
      Send_Agent(zone_id);
      Goto LOOP;
    }
    Update(attack_history);
    break;
}
```

If it finds a malicious behaviour in the neighbouring node, instance of MCA is sent to malicious node only otherwise it sends instance of MCA to all neighbouring nodes. Usually, in the case of flooding attacks, both attacker and relay nodes within the zone show abnormal behaviour. Relay nodes are nodes which forwards flooding packets.

Once the attacker/relay nodes within a particular zone are identified, the MCA reports back to SCA with TTL information. Normally, TTL field should be more at attacker (source) compared to relay nodes. Using this information, SCA can identify the attacker and finally the attack history database (TABLE 2) is updated by the history collection module.

If the attacker is located in a zone other than the estimated zone, the SCA deploys MCA to zone having next highest Psi (n). This process is repeated until the actual attack zone is identified, and finally it updates the attack history database (TABLE 2).

3.7 Countermeasures

Once the attacker's origin is found using the Mobile Cognitive Agent of attacker trace back algorithm and then it can be updated to the Restricted list (TABLE 3) which is present in the Super node with the attacker's MAC address, node number and the number of times the attack has occurred from the same attacker. The MAC address can be found by using the cross layer information as mentioned by yongjinkim in [10].

The victim node is informed the MAC address so that when a packet arrives from that address it can be dropped. When the same MAC address propagates the attack from different zones, the count gets incremented. When the count reaches a particular threshold, the cross layer information of the attacker is passed to all the nodes in the network so that the same node cannot propagate the attack inside the network. The details of the restricted list database are shown in TABLE 3.

Table 3: Restricted List present in Super Node

Node id	MAC Address	Count
12	BE:FE:RF:54:35:A2	14
4	AF:FE:RF:54:35:A2	8
7	FE:48:RF:54:35:A2	10

4. SIMULATION AND RESULTS

The proposed algorithm is simulated using Network Simulator (NS)-2. Mobile agents related simulations cannot be made to run in standard NS package. Since, NS software promotes extension by users; NS package is modified similar to the implementation seen in [16] to include the necessary features.

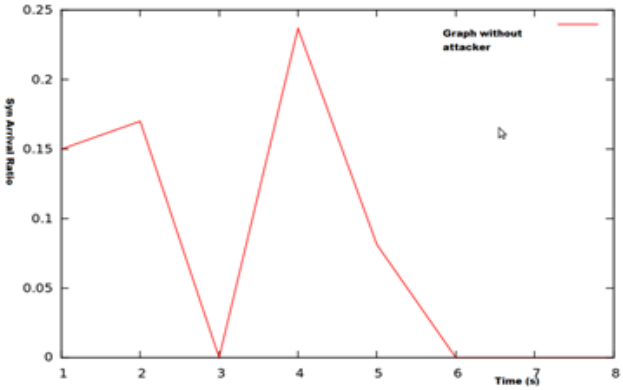

Fig. 3 SAR without attacker

The security of the mobile agents is ensured by the solutions mentioned in [3]. Super node creates and maintains an attacks history database which contains the information of all the attacks originated in the network. DSDV is chosen as a prominent algorithm for the proposed scheme. The experimental setup along with simulation is carried out by framing topological illustration of the network containing 30 nodes in which the radio propagation range for each node is 10 meters. The total simulation time is 30 minutes. In simulation, the attacks are generated artificially from different zones. In flooding scheme, query messages with attack signature are flooded to the entire network.

The SYN Arrival Ratio (SAR) is calculated for the network with and without attacks and is shown in the fig. 3 and fig. 6 respectively. Analysis of results are clearly plotted in Fig.4 & Fig.5 and numerically tabulated in Table 4.

Table 3: Attacker Detection Rate Vs False Positive Rate

TCP segment based attacks	Detection Rate	False Positive Rate
SYN Flood	94%	4%
FIN	93%	3%
RST	100%	1%
URG	100%	1%
ACK	100%	4%
PSH	95%	3%

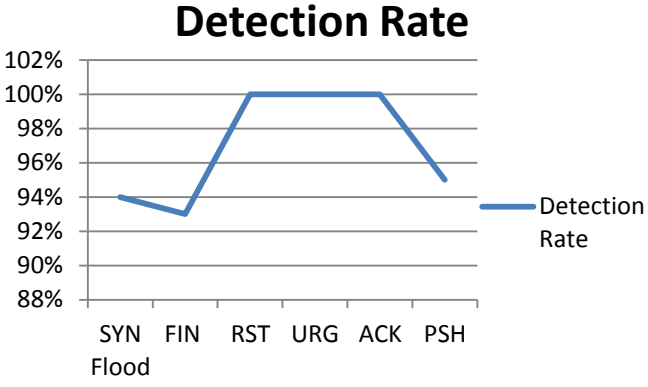

Fig.4. Attack detection rate in TCP segment

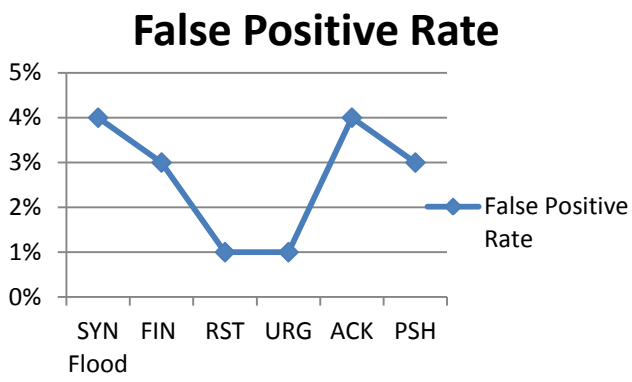

Fig.5. False positive rate in TCP segment

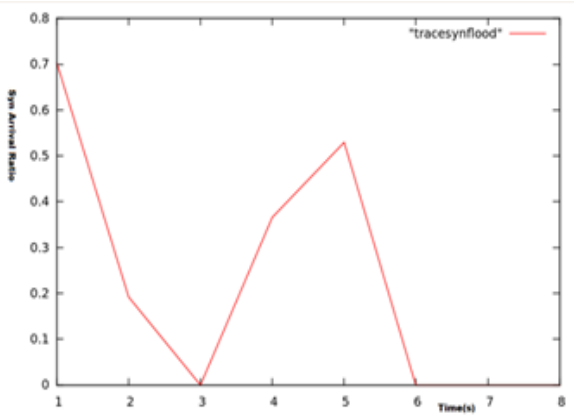

Fig.6. SAR with attacker

Table 5: Comparison of proposed system with existing

Techniques	CATCH[10]	ZSBT[8]	Proposed-MCA
Detection Rate	93.10%	94.1%	96.45%

5. CONCLUSION

In this paper, Tracing of TCP attacker and proper countermeasures for the attacker is proposed using a novel method in MANET environment. The proposed algorithm is more advantageous with low communication and computational complexity compared to the other existing schemes. Damage caused is mitigated by low trace back time and also there is sufficient time available for super nodes for the purpose of countermeasures. From Table 5, it is clearly states the robustness of the proposed method to spoofing attack as the trace back is not based on spoofed IP address and MAC address.

6. REFERENCES

[1] H. Wang, D. Zhang, and K.G. Shin, "Detecting SYN flooding attacks," Proceedings of IEEE INFOCOM, 2002, pp.1530-1539.

[2] Kamanshis Biswas, Md. Liakat Ali, "Security Threats in Mobile Ad Hoc Network", 2007

[3] R. Gill, J. Smith, M. Looi, and A. Clark. "Passive Techniques for De- tecting Session Hijacking Attacks in IEEE 802.11 Wireless Networks". In Proceedings of AusCERT Asia Pacific Information Technology Security Conference (AusCert 2005).

[4] RFC 4987 - TCP flooding attacks and common mitigations.

[5] Seung- won Shin, Ki- young Kim, Jong- soo Jang. "Seung-won Shin, Ki-young Kim, Jong-soo Jang, "D-SAT: Detecting SYN flooding attack by two-stage statistical approach," The Symposium on applications and the Internet, , 2005, pp 430-436.

[6] Y.Ohsita, S.Ata, and M.Murata, "Detecting Distributed Denial-of-Service Attacks by Analyzing TCP SYN Packets Statistically," Proceeding of the IEEE Communications Society Globecom, , 2004, pp. 2043-2049.

[7] Babu BS, Venkataram.P "A dynamic authentication scheme for mobile transactions," International Journal on Network Security 2009, pp.73-112.

[8] X. Jin, Y. Zhang, Y. Pan, and Y. Zhou, "ZSBT: A novel algorithm for tracing DoS attackers in MANETs," EURASIP Journal on Wireless Communications and Networking, vol. 2006, pp 1-9.

[9] S.Savage, D.Wetherall, A.Karlin, and T.Anderson, "Network support for iptraceback," IEEE/ACM Trans. Networking., vol.9, June 2001, pp.103-144.

[10] Y. Kim and A. Helmy, "CATCH: A protocol framework for cross-layer attacker traceback in mobile multi-hop networks," presented at Ad Hoc Networks, 2010, pp.193-213.

[11] N. Nishanth and PallapaVenkatram, "Mobile agent based TCP Attacker Identification in MANET using the Traffic History (MAITH)," International Conference on Communication Technology, 2011, pp.1130-1134.

[12] Vasilios A. SirisyandFotiniPapagalou, "Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks" , in Proc. Of IEEEGlobecom 2004 (Security and Network Management Symposium), Dallas, USA, November 2004, pp.66-81.

[13] Kunal Shah, "Performance analysis of mobile agents in wireless internet applications using simulation", 2003.

[14] CERT Advisory CA-96.21, TCP SYN Flooding and IP Spoofing Attacks, September 24, 1996, pp.200-213.

[15] Yongjin, V. Sankhla, and A. Helmy, "Efficient traceback of dos attacks using small worlds in manet," in 60th IEEE Vehicular Technology Conference, vol. 6, 2004, pp.63-91.

[16] A.Helmy, "Small World in Wireless networks," IEEE Communication Letters, vol.7, No.10, oct 2003, pp.490-492.