SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET

Khalid Hussain
The University of Lahore
Islamabad Campus
Islamabad, Pakistan
khalid@cs.uol.edu.pk

Syed Jawad Hussain
The University of Lahore
Islamabad Campus
Islamabad, Pakistan
jawad.hussain@cs.uol.edu.pk

NZ Jhanjhi
SoCIT, Lakeside campus, Taylor's University
Malaysia
Noorzaman.jhanjhi@taylors.edu.my

Mamoona Humayun
Colege of computer and Information Sciences, Jouf University
Al-Jouf, Saudi Arabia
mahumayun@ju.edu.sa

***Abstract*— SYN flood attack is a very serious cause for disturbing the normal traffic in MANET. SYN flood attack takes advantage of the congestion caused by populating a specific route with unwanted traffic that results in the denial of services. In this paper, we proposed an Adaptive Detection Mechanism using Artificial Intelligence technique named as SYN Flood Attack Detection Based on Bayes Estimator (SFADBE) for Mobile ad hoc Network (MANET). In SFADBE, every node will gather the current information of the available channel and the secure and congested free (Best Path) channel for the traffic is selected. Due to constant congestion, the availability of the data path can be the cause of SYN Flood attack. By using this AI technique, we experienced the SYN Flood detection probability more than the others did. Simulation results show that our proposed SFADBE algorithm is low cost and robust as compared to the other existing approaches.**

***Keywords*—** *SYN Flood Attack, Artificial Intelligence, Bay Estimator, MANET, Probability*

I.ⁿ INTRODUCTION

MANET is addressed as typically a service and never as an infrastructure. Typically, cellphone hosts are dynamically linked and keep on monitoring each other continuously and may post packets at any given time. In MANET, a few cellular phones for WIFI interfaces produce a limited correlation; without the intervention of some sort of neither the arranged infrastructure nor centralized administration. Hosting space from every last cellular node penetration may differ, yet hosts available to each and every other's wide variety must believe in a second computer to the site relay email messages [1]. So, that multi-hop network gets, from where few intermediate nodes and other relays the packets provided with an insight, big number earlier than the attack the site high number. Almost all nodes take advantage of being a router. In a very paid off efforts, the system can be view this bizarre data due to the amount of these servers and clients, the node transmitter/receiver proper protection tendencies, their connecting energy fees, knowing the co-channel agitation fees. Their local community topology can adjust in the period being computers extend not alter the network verbal exchanges but additionally party specifics. So, typically the MANET features based on some salient characteristics [2].

Safe practices are usually a fundamental specialist around wired or even mobile emails. The node arrive at that have been MANET strenuously banks on whether it be its safeness will be sound. However, its ex-elements of most MANET perspective also hassle and choices for accomplishing the network basic safety outlook, for example, the confidentiality, authentication, trustworthiness, easy flip open access, accomplish possession, or even non-repudiation. There are wide varieties of attacks that target the weakness of MANET. For example, routing messages are an essential component of mobile network communications, as each packet needs to be pass quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as DSR, or AODV [3, 4]. More sophisticated and subtle routing attacks have been identified in recently published papers, such as the black hole (or sinkhole) [5], Byzantine [6], and wormhole [7, 8] attacks. Currently routing security is one of the hottest research areas in MANET.

II.ⁿ LETERATURE REVIEW/BACKGROUND

In general, the SYN Flood attack has been categorized into four categories; Router, Server, Agent, and Firewall. To prevent the system from SYN Flood attack, normally every site installs a firewall. Some of the firewall systems available today are SYN Defender and Proxying [6, 9]. Firewall plays a vital role in protecting systems before establishing the connection between a client and the server. Firewall monitors all the TCP based communication between client and server besides monitoring the TCP connection status. Although, this approach is beneficial but it increases the delay due to extra processing. Two more approaches like SYN Cache and Cookies are used in server-based approach. The functionality of the SYN Cache is to keep track of all SYN requests. It also maintains an overall hash matrix for all those incomplete connections with the servers requested by the client. In SYN Cookies, when a server receives that SYN request from the client, it responds by forwarding a SYN/ACK with complete packet information. But SYN cookies add secret seed information with the complete packet information. The server is responsible to evaluate the ACK if the server finds that the received ACK belongs to the previous packet than server will establish the connection and mark its state as established. For SYN Cookies, the server hasn't even tried to verify the half-open connection. To verify half-open connections, a soft agent based three-way handshake monitoring approach for local area network paradigm has been developed for mitigating the SYN Flood attack called

978-1-5386-8125-1/19/$31.00 ©2019 IEEE

Synkill is introduced [10]. Synkill works by monitoring the respective ACK of the SYN for a certain period of time, if that respective ACK will not respond within a period of time then Synkill initiates RST and tear down that half-open connection as well as it releases all the resources occupied by that half-open connection. Another technique known as MLUTOPS has been developed for detecting the bandwidth attack. This technique uses a tree methodology to monitor all the incoming and outgoing packets from each node at different levels of the tree [11]. In Incoming traffic factorization mechanism all incoming traffic is monitored at the entrance of the router and if the source address of the sender packet traces out from any external network then those packets are immediately blocked. This methodology is useful; if, the SYN Flood attack is launched externally, but fails in-case of internal launch [12]. Besides, Distributed Packet Filtering (DPF) offers a better choice of monitoring of distributed and dynamic topology changes, route spoofing and the monitoring the incoming and outgoing traffic from a valid path [13] has the ability to perform it. Although, the above-mentioned methods provide a mechanism to overcome SYN flood attacks but they are not intelligent enough to overcome all the threats. Therefore, this study proposed an AI-based SYN Flood Attack Detection Based on Bayes Estimator (SFADBE) that will avoid overheads and provide robust mechanisms against SYN floods.

III. THE PROPOSED SYN FLOOD ATTACK DETECTION BASED ON BAYES ESTIMATOR(SFADBE)

In this research, an efficient algorithm is proposed to detect SYN flood Attack based on SYN Flood Attack Detection Based on Bayes Estimator (SFADBE) in MANET. In this detection technique, a cluster based environment in MANET has assumed in which every cluster has a Cluster Head (CH), which is responsible for secure communication in the cluster. In SFADBE, every node in the cluster will revoke the certificate for authentication and authorization from CH and CH will issue a signature based certificate to all the nodes in its respective cluster. Every node in that cluster can communicate with each other without asking permission from the CH and will move from one place to another within the cluster. If any node wants to establish a connection outside the cluster, then it will be through CH. In MANET, nodes can move from one place to another place freely. As each node is registered and authorized by the CH; so, nodes can communicate with each other through CH. If, some node becomes compromised and someone becomes victim to SYN Flood attack even though the CH, registers those nodes.

When a node received a beacon message from its neighbor node Nn the neighbor node maintains/updates its routing table about that information without knowing that those nodes are good or bad nodes. A compromised node m can penetrate the cluster and made the other good nodes as malicious nodes and those malicious nodes are formulated as compromised nodes Am. If there are n numbers of SYN attack nodes in the cluster, then it will be n compromised nodes {A1, A2, ……An}. If there will be no effective detection mechanism for detecting those malicious nodes then them acting, as good nodes cannot be detected as malicious. Therefore, to detect these malicious nodes, the SFADBE algorithm is proposed. In the proposed SFADBE algorithm when a node wants to establish a connection with the destination node then there is a requirement to adopt a secure communication path through good nodes. To find out the suspected node the source node gathers the information about the node effected with SYN Flood attack. Figure 1 shows the proposed SFADBE algorithm.

```
Begin SFADBE
        input: m node id
        output: malicious_buffer information
        for mi← 1 to mn – 1 do
            formj←1to mn – 1 do
            ifdif (node mi, mj) <th
            then
            check in the B/W Col
            (mi, mj);
        return routing table
End
```

Fig 1. The Proposed SFADBE Algorithm

In Figure 1, SYN Flood attack detection algorithm is presented in a simple way. In Figure 2, there are eight clusters and a Cluster Head supersedes every cluster. If a node in the cluster performs the malicious activity then the Cluster Head marked that node as Malicious (B_n).

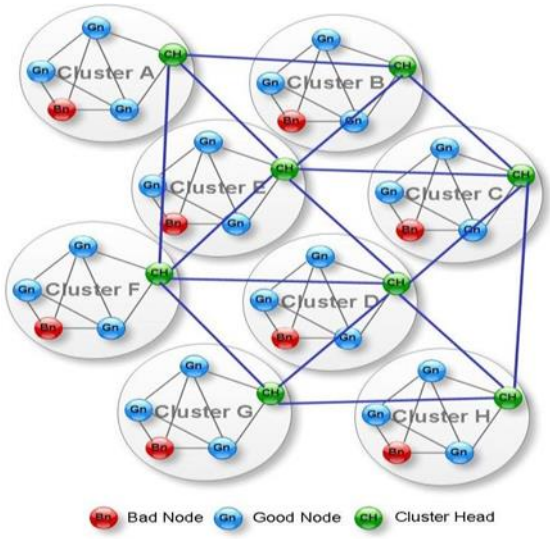

Fig 2. Good and Bad node Cluster Environment

In the presented Clusters, every node is intelligent and able to monitor the malicious activity by its neighbor node; the monitoring node then informs the cluster head about that malicious activity and the cluster head confirms and marks the malicious node as Bn. In Figure 2, only E and H Clusters have no bad nodes. Table 1 shows the bad node detection time in the respective cluster. The marked bad node is affected by SYN Flood attack.

TABLE 1: BAD NODE (BN) DETECTED BY THE CLUSTER HEAD

Time	Cluster A	Cluster B	Cluster C	Cluster D	Cluster E	Cluster F	Cluster G	Cluster H
to	Gn	Gn	Bn	Gn	Gn	Gn	Gn	Gn
t1	Bn	Gn	Gn	Gn	Gn	Bn	Gn	Gn
t2	Gn	Gn	Gn	Bn	Gn	Gn	Gn	Gn
t3	Gn	Bn	Gn	Gn	Gn	Gn	Bn	Gn

IV. SYN ATTACK DETECTION AND IDENTIFICATION METHOD OF SFADBE

The proposed Intelligent SYN Flood Attack detection (SFADBE) model has fairly identified the compromised nodes by SYN Flood Attack and classified those marked nodes in an array Am by using the prescribed procedure.

Step 1: When a node broadcasts the RREQ to find out the Sink node and by using any malicious activity, the neighbor node changes the nature of the RREQ. Source as well as the neighbor node has not received the RREQ again, and then the monitoring neighbor trigger's its Mac Counter, after reaching the threshold level then the monitoring node is marked as malicious in the routing table.

Step 2: When the node is marked as malicious, the broadcasting node checks its B&W list. If another node wants to communicate with the other node in the cluster, then that node broadcast the RREQ again, and then those monitoring nodes exchange its routing table with source node. Source node will find out the update information using Equation (1). R.Ta and R.Tb are the routing tables of previous monitoring Node and current Source Node. When the new Source node, sets its routing table and new receiving routing table, it is possible to find the difference as well as the updated information of any node marked as malicious.

$$Diff(R.Ta, R.Tb = \frac{1}{2}\sum_{i=1}^{2} di \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where d_i = the B&W list

$$di = \begin{Bmatrix} 1 \ldots if R.Ta \neq R.Tb \\ 0 \ldots if R.T0 = R.Tb \end{Bmatrix}$$

Step 3: Here, Bayes Estimator is used to calculate the malicious behavior of the neighboring nodes in the cluster based on binary properties such as;

G_n Good Node
B_n Bad Node

If adjacent node(s) mark the Gn as Bn in the same cluster based on packet drop happening more than the threshold value. In addition, if a node is marked Bn by more than two adjacent nodes in the same cluster. For a significance level, ∞ there is a corresponding reception cluster Ω. The precise consequence level ∞ is distinct as the probability of coloration theory, if it is true and defined as $P(marked \quad B_n / B_n \quad is \quad true) \leq \infty$

In implication testing $Diff(R.T_a, R.T_b)$ is supposed to be the test statistic for judging whether observed data belong to the null-hypothesis or not. If the test statistic $Diff(R.T_a, R.T_b) \in \Omega$,then assumption Bn can be accepted. On the conflicting, if, $Diff(R.T_a, R.T_b) \notin \Omega$ then assumption Bn should be irrelevant. As per the evaluation when $Diff(R.T_a, R.T_b) \geq Threshold$ we advocate the $Diff(R.T_a, R.T_b) \in \Omega$.

Step 4: When a node detects a neighbor node as malicious in a cluster and or another node. The detected node will be classed as Bn. If there are more than two node detected as bad it becomes two set $B_1 = \{B_{n1}, B_{n2}\}, \quad B_2 = \{B_{n1}, B_{n2}\}$ then we can explain those bad nodes as set of $B_1 = \{B_{n1}, B_{n2}, B_{n3}\}$. With this, we not only can identify the bad nodes but also can communicate with the rest of the good nodes to avoid the communication through these bad nodes.

V. COMPUTING THE CONGESTION AND SNR VALUE

The two more important parameters for hampering the quality of service are congestion and SNR. By using the estimation theory, every node can be able to calculate the threshold value of the established link on these basic parameters. In real time traffic management, if an intruder impose a SYN Flood attack on the established link then node can decide whether to continue the communication through established link or not by assumption Gn. The assumption Gn is selected when $Diff(x, y) \geq Threshold$ Where is x = the threshold value of SNR and y is congestion. For fair malicious attack detection and minimizing the wrong detection, an appropriate algorithm can be used for accurate threshold information, which is called false positive detection (Fpd) and false negative detection (Fnd). As per assumption, the wrong malicious node's identification will increase the system detection cost, whereas the right information will improve the system performance with respect to maximizing throughput and minimizing end-to-end delay. Cost function can be calculated with Kay's method.

$$Cost = C_{\max} F_{pd} + C_{\min} F_{nd} \ldots\ldots\ldots (2)$$

Whereas C_{max} and C_{min} are factor of false positive detection and false negative detection error correspondingly. For fair evaluation of the system, consider the equal threat value of the (Fpd) and (Fnd) and constant the C_{max} and C_{min} equal to 1. The values of the cost factor are firm rendering to the explicit application. As illustrated in the Figure 3, the proposed mechanism performance is calculated using Kay's method. The evaluation mechanism of the proposed system shows that by increasing the detection threshold value results in decreasing the probability of false negative detection and increases the false positive detection. In Figure 3, it can be seen that if the threshold is about 8.0 percent of the overall system, the cost is negligible and Fpd gets a comparative stability for a given ∞ value.

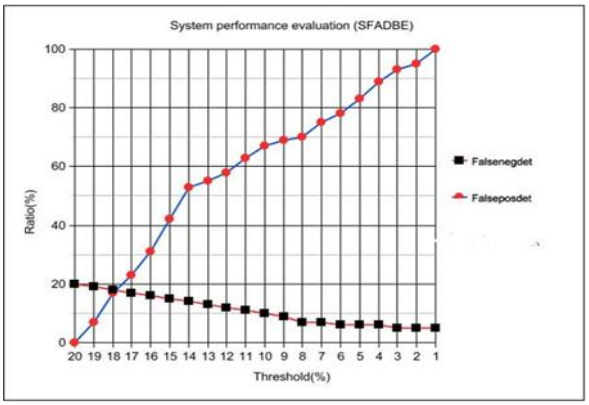

Fig 3.Overall performance of (SFADBE) for false positive detection

VI. CONCLUSION

This paper has proposed an Artificial Intelligence (AI) technique named as SYN Flood Attack Detection Based on Bayes Estimator (SFADBE) for Mobile ad hoc Network (MANET) to detect the SYN flood attack. SYN flood attack takes benefit of the congestion caused by populating a specific route with unwanted traffic that consequently causes the denial of services. In SFADBE algorithm, every node gathers the available channel's information, SAFDBE then selects a secure and congested free channel for the traffic. By using this technique, we experienced the proposed detection technique for SYN flood attack probability more than the others did. Simulation results shows that our proposed SFADBE algorithm is low cost and robust as compared to the other existing approaches. The SFADBE is efficient in detecting attack in a timely manner before the destruction of the network services. In future, the proposed algorithm will be enhanced for further improvement in the SYN flood prevention and bandwidth issues in MANET.

REFERENCES

[1] Stuntebeck, Erich. "Securing Relayed Email Communication." U.S. Patent No. 20,160,094,522. 31 Mar. 2016.

[2] Jim, Lincy Elizebeth, and Mark A. Gregory. "A review of artificial immune system based security frameworks for MANET." International Journal of Communications, Network and System Sciences 9.1 (2016): 1.

[3] Jain, Aaditya. "Performance Analysis of DSR Routing Protocol With and Without the Presence of Various Attacks in MANET." International Journal of Engineering Research and General Science 4.1 (2016).

[4] Patel, Kajal S., and J. S. Shah. "Study the Effect of Packet Drop Attack in AODV Routing and MANET and Detection of Such Node in MANET." Proceedings of International Conference on ICT for Sustainable Development. Springer Singapore, 2016.

[5] Badenhop, Christopher W., Benjamin W. Ramsey, and Barry E. Mullins. "An Analytical Black Hole Attack Model Using a Stochastic Topology Approximation Technique for Reactive Ad-Hoc Routing Protocols." International Journal of Network Security 18.4 (2016): 667-677.

[6] Yu, Ming, Mengchu Zhou, and Wei Su. "A secure routing protocol against byzantine attacks for MANETs in adversarial environments." IEEE Transactions on Vehicular Technology 58.1 (2009): 449-460.

[7] Jhaveri, Rutvij. H "MANET routing protocols and wormhole attack against AODV." International Journal of Computer Science and Network Security 10.4 (2010): 12-18.

[8] Imran, Muhammad, Farrukh Aslam Khan, Tauseef Jamal, and Muhammad Hanif Durad. "Analysis of Detection Features for Wormhole Attacks in MANETs." Procedia Computer Science 56 (2015): 384-390.

[9] Ambrosin, Moreno, Mauro Conti, Fabio De Gaspari, and Radha Poovendran. "Lineswitch: Efficiently managing switch flow in software-defined networking while effectively tackling dos attacks." In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, pp. 639-644. ACM, 2015.

[10] Bellaiche, Martine, and Jean-Charles Gregoire. "SYN flooding attack detection based on entropy computing." In Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, pp. 1-6. IEEE, 2009.

[11] Bhuyan, Monowar H., Hirak Jyoti Kashyap, Dhruba Kumar Bhattacharyya, and Jugal K. Kalita. "Detecting distributed denial of service attacks: methods, tools and future directions." The Computer Journal (2013): bxt031.

[12] Song, Yunlong, Min Liu, Shaojie Tang, and Xufei Mao. "Time series matrix factorization prediction of internet traffic matrices." In Local Computer Networks (LCN), 2012 IEEE 37th Conference on, pp. 284-287. IEEE, 2012.

[13] Park, Kihong, and Heejo Lee. "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets." In ACM SIGCOMM computer communication review, vol. 31, no. 4, pp. 15-26. ACM, 2001.