International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-4,April 2016
ISSN: 2395-3470
www.ijseas.com

Cross layer Link Quality Assessment Based Flooding Attack Detection and Prevention in Mobile Ad hoc Network

Ms.Afroze Ansari
Research Scholar, Dept of Computer Science & Engg
VISVESVARAYA TECHNOLOGICAL UNIVERSITY
Regional Office, GULBARGA
KARNATAKA, INDIA

Dr. Mohammed Abdul Waheed
Associate Professor, Dept. Computer Science & Engg.
VISVESVARAYA TECHNOLOGICAL UNIVERSITY
Regional Office, GULBARGA
KARNATAKA, INDIA

Abstract
Mobile Ad hoc Network (MANET) is one of the most popular dynamic topology reconfigurable local wireless network standards. Mobile nodes in MANET may join or leave the network on-the fly. Nodes manage the network in a distributed way and there is no centralized control over the topology. Due to dynamic nature of the network, MANET is extremely vulnerable to security threats. Distributed Denial of Services(DDoS) is one of the most challenging threats in such a network. Flooding attack is one of the forms of DDoS attack whereby certain nodes in the network miss-utilizes the allocated channel by flooding packets with very high packet rate to it's neighbors, causing a fast energy loss to the neighbors and causing other legitimate nodes a denial of routing and transmission services from these nodes. In this work we propose a novel link layer assessment based flooding attack detection and prevention method. MAC layer of the nodes analyzes the signal properties and incorporated into the routing table by a cross layer MAC/Network interface. Network layer analyzes the statistical properties of the change in the parameters and detects flooding nodes based on relative high channel acquisition by nodes with low power signals. Once a node is marked as a flooding node, it is blacklisted in the routing table and is communicated to MAC through Network/MAC cross layer interface. MAC layer of a node does not exchange any RTS/CTS packet with the blacklisted nodes, thereby completely isolating the flooding node. Results shows that the proposed technique produces more accurate flooding attack detection in comparison to current state of art statistical analysis based flooding attack detection by network layer.
Keywords: MANET, Flooding Attack, DDoS, Cross Layer

Introduction

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. A **mobile ad hoc network** (**MANET**) is a self-configuring infra structure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

Distributed denial-of-service attack (**DDoS attack**) is an attempt to make a machine or network resource unavailable to its intended users. MANET is a distributed system that comprises wireless mobile nodes that can freely and dynamically self-organize into arbitrary, temporary, and ad hoc network topologies, allowing seamless interconnections without pre-existing communication infrastructure and central administration.Due to its unique characteristics, MANET is vulnerable to various security threats, and it is particularly susceptible to the DDoS attack.

DDOS ATTACKS IN MANETS : Distributed denial of Service attacks usually occurs in MANETS or in wireless networks. It is an attack where multiple systems comprised together and target a single system causing a denial of service (DoS). The target node is flooded with the data packets that system shutdowns, thereby denying service to legitimate users. The services under attack are those of the “primary victim”, while the compromised systems used to launch the attack are often called the “secondary victims.” Current MANets are basically vulnerable to two different types of DDoS attacks:

i) *Active DDoS attack* is an attack when misbehaving node has to bear some energy costs in order to perform the threat.
ii) Passive DDoS attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly.

Nodes that perform active DDoS attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive DDoS attacks with the aim of saving battery life for their own communications are considered to be selfish . The attacks are classified as:

Modification Attack: Modification is a type of attack when an unauthorized party not only gains access to but tampers with an asset.

Impersonation Attacks: As there is no authentication of data packets in current ad hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing.

Fabrication Attacks: Fabrication is an attack in which an unauthorized party not only gains the access but also insert.

In this work we model a Mobile Adhoc Network that implements geographic cluster based routing. As Cluster heads services to several nodes in a given area in a network, these nodes are extremely vulnerable to security threats. A DDoS attack on cluster head nodes may result in void area in a network and may ultimately affect the routing and data transmission over entire network.

2. **Relatad Work**

Annamalai, Arunmozhi [1] focuses on mobile ad hoc network's routing vulnerability and analyzes the network performance under two types of attacks, flooding attack and black hole attack that can easily be employed against the MANETS . Defense scheme against RREQ flooding attack based on binary exponential backoff and RREQ_RATELIMIT was proposed. They have developed a NRMT scheme for MANETs that is resistant to the black hole attack. The scheme identifies the attacker based on timing information and destination sequence number. Hence a secure routing is provided with the proposed solution.

Priyadharshini, V [2] proposed a new cracking algorithm to stop that DDOS attacks. The algorithmic design a practical DDOS defense system that can protect the availability of web services during severe DDOS attacks. The proposed system identifies whether the number of entries of client exceeds more than five times to the same sever, then the client will be saved as a attacker in blocked list and the service could not be provided. So the algorithm protects legitimate traffic from a huge volume of DDOS traffic when an attack occurs. When a DDoS attack occurs, the proposed defense system ensures that, in a web related server information are managed without corruption. This newly designed system that effectively gives the availability of web services even during severe DDoS attacks.

Ming, Yu[3] focuses on exploring the feasibility of mitigating flooding-based DDoS attacks by queueing disciplines. A comparative study is made between SFQ and FCFS (First Come First Served) on their efficacy and robustness in mitigating UDP flooding, a typical flooding-based DDoS attack.SFQ is more efficient and more robust when its parameter buckets is larger than or approximately equal to the number of network flows.

Sharma et al [4] shows the effect of DDoS in routing load, packet drop rate, end to end delay, i.e. maximizing due to attack on network. And with these parameters and many more also build secure IDS to detect this kind of attack and block it. The proposed mechanism protects the network through a self organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbors. After a period of time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a good network performance in terms of security as compare with attack case.

Kumar, Mukesh[5] proposed a scheme that is distributed in nature it has the capability to prevent Distributed DoS (DDoS) attack. It was found that flooding based DDoS attack have greater impact on network performance i.e. network performance decreases more in case of flooding attack. By implementing IP broadcast disable technique it was found that proposed prevention technique is better than existing techniques. Packet delivery ratio becomes doubles and number of collisions reduced to half by using proposed prevention technique under different number of attackers.

Khan, Rizwan[6] proposed the detection and control mechanism for DDOS attacks over reputation and score based MANET and a clustering technique that uses the reputation and score value of nodes. this work provides an incentive or credit based mechanism that can provide cooperation among nodes in the network and improve overall network performance and functionality by prevention, detection and control of DOS and DDOS attacks.

Bhange[7] discusses a statistical approach to analysis the distribution of network traffic to recognize the normal network traffic behavior.. They has also discussed flooding attacks. The EM algorism is discussed to approximate the distribution parameter of Gaussian mixture distribution model. Another time series analysis method is studied. A method is used to recognize anomalies in network traffic, based on a non restricted α-stable model and statistical hypothesis testing.

Devi[8] proposes a detection scheme based on the information theory based metrics. The proposed scheme has two phases: Behaviour monitoring and Detection. In the first phase, the Web user browsing behaviour (HTTP request rate, page viewing time and sequence of the requested objects) is captured from the system log during non attack cases. Based on the observation, Entropy of requests per session and the trust score for each user is calculated. In the detection phase, the suspicious requests are identified based on the variation in entropy and a rate limiter is introduced to downgrade services to malicious users. Based on the information metric of the current session and the user's browsing history, it detects the suspicious session. Once detected, a rate limiter and a scheduler are used to downgrade service to the malicious users and to schedule the less suspicious session based on the system workload and the user's trust level.

Sharma[9] aim is seeing the effect of DDoS in routing load, packet drop rate, end to end delay, i.e. maximizing due to attack on network. And with these parameters and many more also we build secure IDS to detect this kind of attack and block it. The results demonstrate that the presence of a DDOS increases the packet loss in the network considerably. The

proposed mechanism protects the network through a self organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbors. After a period of time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a good network performance in terms of security as compare with attack case.

Bala[10] proposes a bottom up detection and prevention techniques for DDoS in MANET thereby achieving an efficient quality of services provisioning. Our method relies on the use of monitoring and measurement techniques to evaluate the impact of SYN flooding attacks. This approach can accurately identify the SYN flooding DDoS attack and consequently applying window control to reduce congestion and TTL based packet filtering technique to identify attacker and blacklist that attacker.

3. Proposed Work

There are various techniques and mechanisms proposed for flooding attack detection and prevention in wide range of wireless networks. Most of the techniques relies upon the statistical analysis and the properties of the packets. As the flooding attack is essentially a tool to block legitimate bandwidth and session of the nodes, most of the existing systems relies on network layer detection for intrusion and flooding attack.

However, a flooding attack can be carried out at any layer, starting from application data flooding to MAC control packet flooding. No matter, at which layer the attack is carried out, the purpose of such attack always remain to deny the nodes with their deserving data service. MANET being a self configuring network, needs nodes to dynamically manage the routes in distribute ways. Thus, existing literature argues and models such attack in Network layer.

However, in principle, once a malicious nodes starts flooding the packets, there are other characteristics that needs to be taken into account.

For example a flooding node will lose tremendous amount of power for flooding the packets. Thus, generally such attacks are modeled through low power packets. As the goal of the malicious nodes is not to send any valid data, rather to block the resources of the attacked node, the attacker attempts to conserve energy by generating low power data. Such data then obviously have very high bit error rate and low signal to noise ratio. Hence SNR and BER can be considered as significant identity of an attack signature.

Further, an attacker node needs huge channel share for carrying out the flooding attack. It needs to request for a channel access by generating RTS packet to it's neighbors. In an attack scenerio, demand for greater channel access would result in high rate of RTS transmission which will ultimately result in high buffer overflow at the receiver nodes. An attacker may also manipulate backoff timer to flood RTS packets.

In another form of attack, an attacker if not responded with CTS packets may generate garbage signals at the physical layer with a sole purpose of jamming the signals of the other nodes.

Hence it is clear that though the ultimate goal of a flooding attack is to deny resources to the MANET nodes, the attck may be modeled at different layers and may have wide range of signatures, starting from signal level signatures to packet level signature.

Hence, a cross layer based technique by means of which different abstract layers can collaborate and participate in attack detection is better suited for MANET.

The proposed work uses this argument to present a layer collaborative non-distributed model for detection of flooding attack in MANET.

Firstly nodes forms a random topology network which is divided into square grids. We assume that nodes know their microlocation while forming the topology. Nodes in a grid collaboratively select a node as clusterhead. Cluster head nodes are predominantly selected based on high degree of connectivity and higher remaining energy.

Any node may communicate with any other node in the network with a reactive Cluster based AODV routing where source node is serviced by the cluster head close to it and a route till the destination is formed through the cluster heads. In case of a cluster head being energy exhausted, an alternative clusterhead is selected locally into the region and route is repaired through the locally modified clusterhead node.

An attack node can either be an outsider or even part of the network. Detection of the attackers that are not registered with the current network is comparatively easy through their MAC address. Therefore we offer a solution for In-Network attacker.

In our simulation an attack node is registered with the current network just like other attack nodes. In every simulation, we consider only one attacker node which randomly chose a clusterhead and floods the cluster head.

Once the clusterhead is formed in an area, the cluster head broadcasts it's id to it's neighbors. Clusterhead ID is updated in the routing table. As the attacker node is also part of this network and located in any of the regions, he also gets the clusterhead id of the region. We randomly model an attacker node to attack any of the active cluster heads that are servicing one or more path. In that way, the risk of the attack is much more severe. When the attack is undetected, it is seen that packet delivery ratio in a path drops significantly.

This justifies both our attacker-attack modeling and proposed technique design.

4. Methodology

Network Topology: We assume a grid topology for the proposed work. Nodes between 10-80 are randomly placed in the network. The topology is divided into four sub region with equal geographic dimensions.

International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-4,April 2016
ISSN: 2395-3470
www.ijseas.com

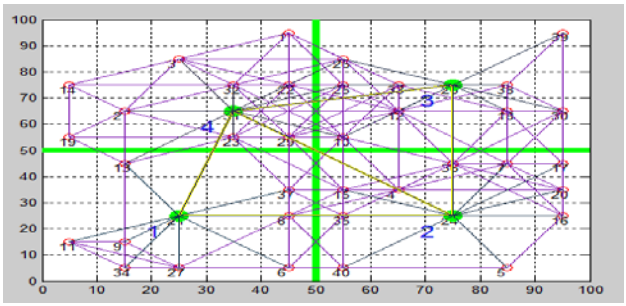


Fig. 4.1 MANET showing nodes ,clusters and cluster head

Radio Model: We assume a Class 1 Bluetooth radio as physical layer model with 100 m maximum transmission and reception range. Nodes transmit with 100mW power. We assume that the attacker node transmits at a much lower power, reducing the transmission range. A Class 2 bluetooth signal emulation allows the attacker to transmit with 2.5mW of power within 10m range which is sufficient for the attacker to broadcast attack signal to a single cluster head node.

Cluster Formation: Nodes first exchange HELLO message with it's neighbors. The HELLO message is updated to incorporate the energy level of the nodes. One of the nodes in an area randomly generates CLUSTERHEAD selection packet by putting it's own id and number of neighbors and broadcasts to all it's neighbors. If a node has more number of one hop neighbors connected to it, it replaces the cluster head id with it's own id and number of neighbor field with it's own number of neighbors from it's routing table. After a TIME_TO_LIVE elapse of the first generated packet, the node number in the cluster head id is selected as the current cluster head and whichever node observes the TTL elapse notifies the cluster head node. Cluster head marks itself as clusterhead and broadcast an JOIN_CLUSTER message with high opower for the packet to reach every node in the area. Upon receiving the JOIN_CLUSTER message, nodes in that are joins the cluster.

Routing Model: We model our routing mechanism based on [19]

Attack Model: A clusterhead, which is part of the current transmission path is selected as the attacked node. An attacker is selected randomly from the nodes nearer to the clusterhead which is not part of the path.
We assume two types of attacks: MAC layer flooding attack and routing layer flooding attack. In a MAC flooding attack, nodes flood the clusterhead with frequent RTS packets demanding for larger channel share. In Routing attack, a node may frequently broadcast route request or increase the HELLO packet. Hence a large part of the time of the cluster head will be busy in servicing the attacking node.
Detection Model: The detection model is based on the statistical analysis of the received packet. It combines the observations of the MAC layer and Network layer to build a attack signature detection. MAC upon receiving any signal calculates the signal strength, BER (from parity check) and calculates SNR (from BER and received signal strength). This information is mitigated to network layer along with the packet (if the packet is forwarded to network layer). When PACKETS are dropped at the MAC layer (non broadcasting and packets that are not intended for the current node) MAC layer extracts the statistic and forwards it to Network layer without any data component.
MAC also forwards the RTS rate and CTS information to Network layer as and when they are received and replied respectively. Thus Network layer maintains an active database with following structure. The database here is called STAT_TABLE.

NodeId	NW_CONTROL RATE	DATA RATE	SNR	BER	RECEIVED POWER	RTS RATE	DELAY	BW

Only cluster head nodes are attacked. However, as the cluster heads may get changed during the course of the communication, all the nodes maintains this table.
NW_CONTROL_RATE- Number of Network layer Control packets par second
DATA_RATE- Number of Data Bits Par Second
SNR- Effective signal to noise ratio of a Node in dB
BER - Number of observed errors par 1000 bits (data or control) received from a node
RECEIVED POWE- Received signal strength from a node in mW
RTS_RATE- Number of RTS packets received par second
DELAY - Network latency in ms, calculated as the timestamp difference between received and transmitted time of a packet.
BW- Effective bandwidth usage in bps by a node calculated at the MAC layer.

Periodically the nodes calculate following statistics of all the parameters:
Statistics={Mean, Standard Deviation, Variance, Entropy}(STAT_TABLE) and the record is logged in another table called OBSERVATION_TABLE.
If at any observation instance current observation parameters are found to be varying more than 50% over the previous time instance observation for any node, then the node is marked as SUSPICIOUS node. If number of STAT_TABLE entries of a SUSPECIOUS node is 30% higher than average number of records from other node than the SUSPECIOUS node is sent a WARNING packet. If the node's bit rate doesn't drop and node continues to flood the cluster head with packets then it is finally marked as BLACKLISTED.

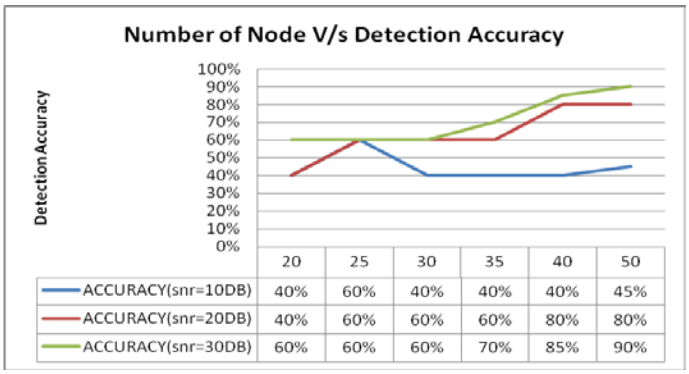
This is essential to account for the variations due to topology changes like node mobility, network congestion and so on. Once a node is blacklisted, it is not allocated any channel by MAC layer and all the subsequent packets being received from this node(Network or MAC packets) are dropped. The BLACKLISTED node's STAT_TABLE entry is deleted, but OBSERVATION_TABLE entry that had triggered the suspicion is stored in another database called SIGNATURE_TABLE. Signature table helps detecting future

International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-4,April 2016
ISSN: 2395-3470
www.ijseas.com

attack quickly. Once a node is blacklisted, it's ID is mitigated to all the neighbors through a special Network layer control packet called BLACKLIST_NOTIFICATION. BLACKLIST_NOTIFICATION packets are mitigated over the entire network (in all the regions so that to isolate the attacker from all future communication).
By dividing the detection into multiple stages and by introducing a WARNING packet, the network provides an option for the attacking node to stop the attack. This serves an alternative purpose too. If in case a node is wrongly marked as BLACKLISTED, it will be unable to participate in any further communication. A WARNING based system gives enough opportunity for misdetection to be rectified.

5. Results

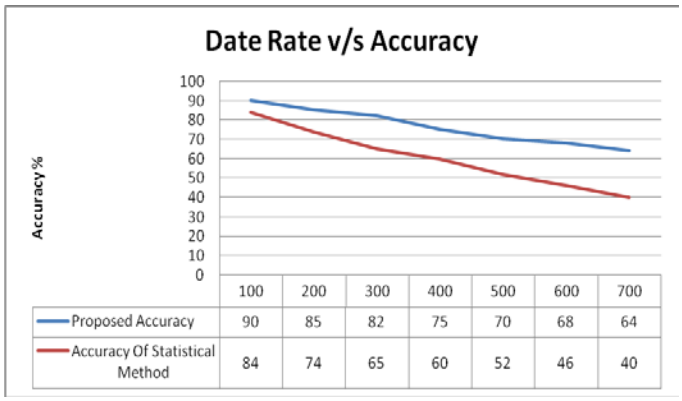
The proposed work is simulated in Matlab. A MANET simulator is created in Matlab with layer wise abstraction of the operation. Further, in every layer, various operations like Routing, Packet Transmission, Statistics Observation, Attack, Detection are modularized. Signal level simulation is carried out with free space radio model and Random way point mobility model.
Number of nodes is varied and detection accuracy is observed in the first experiment. The aggregated result is presented in following figure.



	20	25	30	35	40	50
ACCURACY(snr=10DB)	40%	60%	40%	40%	40%	45%
ACCURACY(snr=20DB)	40%	60%	60%	60%	80%	80%
ACCURACY(snr=30DB)	60%	60%	60%	70%	85%	90%

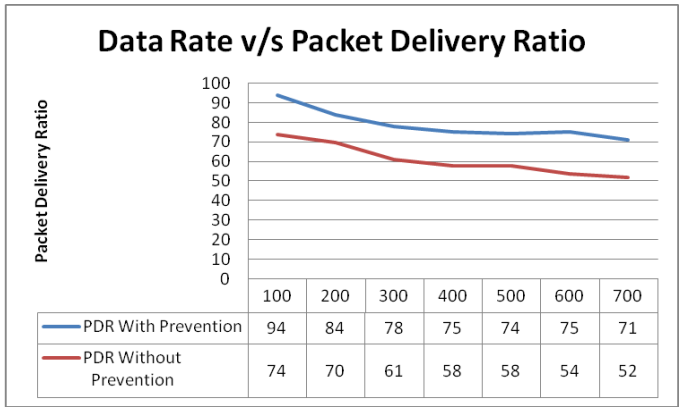
Further we observed the performance under different signal to noise ratio. We observed that under low signal to noise ratio the OBSERVATION-TABLE varied a lot which resulted in low detection accuracy.
We repeated the experiments ten times and calculated the true positive and true negative every time. Total number of correct detection of the attacking node was used for calculating the accuracy. Four sets of experiments were conducted and average accuracy was tabulated for analysis.

In the next experiment, we compared the accuracy of Current Network Layer based statistical method for flooding attack detection with the proposed attack. The RTS and MAC layer attack was undetected by the present state of art. We varied the data rate in 100 Kbps and observed that low to moderate data rate results in better detection accuracy.We also observed that effect of flooding attack is minimum when data rate is high. This is because less bandwidth (and channel) is allocated to nodes which are not part of the route.



	100	200	300	400	500	600	700
Proposed Accuracy	90	85	82	75	70	68	64
Accuracy Of Statistical Method	84	74	65	60	52	46	40

Further we simulated two criteria: One where the attacking node is blacklisted and isolated from the network and another scenario where detection was switched off allowing the attacking node to keep preventing resource allocation to legitimate nodes. The results are as shown below.

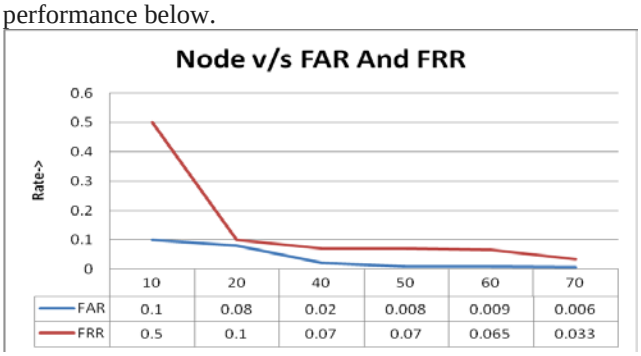


	100	200	300	400	500	600	700
PDR With Prevention	94	84	78	75	74	75	71
PDR Without Prevention	74	70	61	58	58	54	52

Results shows that packet delivery ration in MANET improves significantly when attack prevention is adopted. We observed that increase in data rate resulted in decrease in packet delivery ration in a network even without any attack. Under high data rate, and node mobility, packets took more time to arrive in destination and the route and link quality varied widely resulting in congestion and packet drop. But when preventive model is compared with non preventive model, we see that the preventive model helps to improve the PDR significantly in comparison to non preventive model. This is because once the attack was tracked and the attacking node was isolated, clusterheads have more bandwidth for allocating to the communicating nodes.

We accumulated the results carried out in all above cases of four sets of experiments with ten iterations each and found out the number of times a node was rejected as attacking node when it was actually attacking. We call the ratio of total rejection of attacking node with total instances of simulation as false rejection.

We carried out another set of experiment where we did not incorporate any attack, rather randomly varied the packet rate and the HELLO, RTS packets. We calculated the number of times a node is marked as attacker even when it is not. We call the ratio of total node falsely accepted as attacker to the total simulation instance as false acceptance rate. We compared false acceptance rate with false rejection rate and present the performance below.



	10	20	40	50	60	70
FAR	0.1	0.08	0.02	0.008	0.009	0.006
FRR	0.5	0.1	0.07	0.07	0.065	0.033

We can see from the result that the probability of a node being falsely blacklisted is very low in comparision to the probability of not detecting the attacking node. This is a very important marker of the quality of the performance of the proposed technique. As attack non detection results in only loss of packet delivery ration where as the false implication of a node result in isolating a node from further communication, a low FAR is extremely desired.

Above performance analysis clearly demonstrates the need and effectiveness of the proposed system to protect the network from flooding attack and helping achieve high QoS.

6. Conclusion

MANET's popularity and increased adoptability has increased the threat vulnerability of such network. Due to inherent, less secured environment of wireless networks in comparison to their wired equivalent the threat effect increases. Result section clearly shows that lack of defence mechanism against flooding attack results in drop in packet delivery ratio. Existing network layer based monitoring techniques are not effective in detecting MAC layer specific attacks. Therefore in this work we have proposed a cross layer based mechanism for flooding attack detection with statistical modeling technique. Our non distributed and node centric detection ensures that the detection overhead is minimum. The technique can also detect flooding attack generated from different layers. One of challenges that we observed in the proposed system is drop of accuracy under low signal to noise ratio and node density. Lower node density prevented a good statistical model where as low SNR resulted in huge variation in all other statistical parameters. A future work can be designed to address these issues and solve the puzzle of inaccurate detection under lesser statistical evidences.

References

[1] Annamalai, Arunmozhi “Secured System against DDoS Attack in Mobile Adhoc Network”

[2] Priyadharshini, V., and K. Kuppusamy. "Prevention of DDOS Attacks using New Cracking Algorithm." International Journal of Engineering Research and Applications 2.3 (2012): 2263-2267.

[3] Ming, Yu. "Mitigating Flooding-Based DDoS Attacks by Stochastic Fairness Queueing." Advances in Information Sciences & Service Sciences 4.6 (2012).

[4] Sharma, Prajeet, Niresh Sharma, and Rajdeep Singh. "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network."International Journal of Computer Applications 41.21 (2012): 16-21.

[5] Kumar, Mukesh, and Naresh Kumar. "Detection and Prevention of DDOS Attack in MANET’S Using Disable IP Broadcast Technique." International Journal of Application or Innovation in Engineering & Management (2013).

[6] Khan, Rizwan, and A. K. Vatsa. "Detection and control of DDOS attacks over reputation and score based MANET." Journal of Emerging Trends in Computing and Information Sciences 2.11 (2011).

[7] Bhange, Anup, Amber Syad, and Satyendra Singh Thakur. "DDoS Attacks Impact on Network Traffic and its Detection Approach." International Journal of Computer Applications 40.11 (2012): 36-40.

[8] Devi, S. Renuka, and P. Yogesh. "Detection Of Application Layer DDos Attacks Using Information Theory Based Metrics." CS & IT-CSCP 10 (2012).

[9] Sharma, Prajeet, Niresh Sharma, and Rajdeep Singh. "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network."International Journal of Computer Applications 41.21 (2012): 16-21.

[10] Bala, Laxmi, and A. K. Vatsa. "Quality based Bottom-up-Detection and Prevention Techniques for DDOS in MANET." International Journal of Computer Applications 55.2 (2012): 12-19.

[11] Patel, Mitesh, Shantanu Sharma, and Divya Sharan. "Detection and Prevention of Flooding Attack Using SVM." Communication Systems and Network Technologies (CSNT), 2013 International Conference on. IEEE, 2013.

[12] Bandyopadhyay, Alokparna, Satyanarayana Vuppala, and Prasenjit Choudhury. "A simulation analysis of flooding attack in MANET using NS-3."Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on. IEEE, 2011.

[14] Ibrahim, Mohamed M., Nayera Sadek, and M. El-Banna. "Prevention of flooding attack in wireless ad-hoc AODV-based networks using real-time host intrusion detection." Wireless and Optical Communications Networks, 2009. WOCN'09. IFIP International Conference on. IEEE, 2009.

[15] Balakrishnan, Venkat, et al. "Mitigating flooding attacks in mobile ad-hoc networks supporting anonymous communications." Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on. IEEE, 2007.

[16] Chouhan, Ms Neetu Singh, and Ms Shweta Yadav. "Flooding Attacks Prevention in MANET." International

Journal of Computer Technology and Electronics Engineering (IJCTEE), ISSN (2011): 2249-6343.
Meher, Ruchita, and Seema Ladhe. "Review Paper on Flooding Attack in MANET." International Journal of Engineering Research and Applications(2014): 39-46.
[17] Bhalodiya, Shruti, and Krunal Vaghela. "Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol."International Journal of Computer Applications 125.4 (2015).
[18] Bhuvaneshwari, K., and A. Francis Saviour Devaraj. "Examination of Impact of Flooding attack on MANET and to accentuate on Performance Degradation." International Journal of Advanced Networking and Applications4.4 (2013): 1695.
[19]Xu, Kaixin, and Mario Gerla. "A heterogeneous routing protocol based on a new stable clustering scheme." *MILCOM 2002. Proceedings*. Vol. 2. IEEE, 2002.