ANP- Adaptive Node Profile Based Detection Mechanism For Flooding Attack In MANET

Bhuvaneshwari .K
Scholar, Department of Information Science Engineering, Oxford College of Engineering, Bangalore, India

Dr. A. Francis Saviour Devaraj
Professor, Department of Information Science Engineering, Oxford College of Engineering, Bangalore, India

Abstract

Mobile Adhoc Networks (MANET) are particularly vulnerable to security attacks because of their dynamic topology. The main challenge in MANET is to design the robust security solution that can protect MANET from various routing attacks. Flooding attack is a kind of Denial of service (DOS) attack which is distributive in nature and can exhaust the victim's network of resources such as bandwidth, energy, computing power etc. A node profile based detection mechanism is proposed to detect the flooding attack on MANET using Adhoc on Demand Distance Vector (AODV) routing protocol. The proposed ANP solution and its effectiveness to detect and isolate the malicious node are studied in this paper. For simulating the attack and to study the network parameters java network simulator jist/swans are used.

Index Terms—**AODV, DOS, Flooding attack, MANET, Node Profile.**

1. Introduction

A Mobile Adhoc Network (MANET) is a collection of mobile/semi-mobile nodes with no pre-established infrastructure, forming a temporary network. Each of the nodes has a wireless interface [1] and communicates with its neighbors who are all in its coverage range. Source can reach destination through one or multiple hop. The Ad Hoc On-Demand Distance Vector(AODV) routing protocol enables multi-hop routing between participating mobile nodes wishing to establish and maintain an ad-hoc network.AODV [2] is reactive since it does route request only when needed and does not require nodes to maintain routes to destination that are not actively used in communications.

Flooding attack in MANET is a more concealed form of DOS [3] attack which is produced by the unintentional failure of nodes in the network or by malicious action. This flooding attack can cause severe degradation in network performance. The main intention of a flooding attack is to interrupt the services given to legitimate users by targeting the resource at the victim node or the network. By consuming the resources like bandwidth, battery power etc attacker can set up the denial of service to the end user. In flooding attack the bogus control packets are flooded into the network targeting the victim or the network as a whole. AODV is particularly vulnerable to flooding attack because of its route discovery scheme where the RREQ control packets are broadcasted to all one hop neighbors for finding the path to the destination. Bogus RREQ packets can be disseminated targeting the destination or network and consume the network resources thereby degrading the network performance [4].

In the proposed ANP approach, every node is set with a profile in order to encounter the distributed attack. The proposed ANP has its profile values set based on the behavior of MANET. It identifies the attack and tries to isolates it whenever the node tries to cross the defined threshold value. This threshold value is made adaptive based on the average request allowed in the network. Furthermore, another distinguishable contribution made by this ANP is that it can identify the attack impact as early as it gets started.ANP approach can also isolate the attack traffic(traffic due to RREQ sent by malicious node) by isolating the malicious node from participating in the network.

This paper is organized as follows: Section 2 explains how RREQ flooding attack can be launched and its effects in MANET. Section 3 presents the related work done to detect and prevent the flooding attack in MANET. Section 4 explains the proposed system Section 5 describes the attack model used for study, simulation study of proposed ANP detection mechanism and its result analysis. Section 6 explains the conclusion and future work.

IJERT
IJERT

2. RREQ flooding and its effects

AODV is a reactive routing protocol and it establishes route on demand. It has limit of how much RREQ can be originated by a node. The default value of RREQ_RATELIMIT [6] is 10 as proposed by RFC 3561.The malicious node can override the limit by increasing or disabling it [5]. It can do so because the node has self-control over this rate limit parameter. By this way the malicious node can flood the network with fake RREQs and lead to a kind of DOS attack. In this type of DOS attack the genuine nodes cannot serve other nodes due to the load imposed by fake RREQs. Bandwidth consumption [6, 7] is increased as more number of RREQs is flooded in the network which would otherwise be used by genuine nodes. RREQ packets have high priority than data packets. As the nodes keep on processing the RREQs in spite of data packets there is an overhead in terms of nodes processing time. The routing table entries are created more by the fake RREQs in order to reach destination. Greater amount of network resources like bandwidth are wasted by trying to find routes to destination which do not exist or the routes which are not going to be used for any data communication. This can have very adverse effects in real time applications.

3. Related Work

In Trace back scheme [8] any single packet is traced back to its origin with the help of special router in the network which cooperate with each other. However this method is based on assumption that network topology does not change which will not hold good for MANET. Further they require centralized equipment which is not practically feasible in MANET.

In cooperation enforcement scheme we have credit based scheme and reputation based scheme. The Reputation based model [9] use the nodes reputation to establish the connection. Nodes with high reputation value alone are considered to forward the packets towards destination. Here the malicious nodes are only excluded from forwarding the packets whereas they can act themselves as a source targeting the network by sending fake RREQ's. The credit based model [10] treats the packet forwarding task which has to be charged based on the credit (past history) they earn in the network. They use tamper resistant hardware or virtual bank which requires a trusted third party services to nodes in the network.

In specification based detection mechanism [11] the nodes are monitored for the correct execution with respect to defined constraints. The constraints defined cannot be varied dynamically in case of change in topology which is more common in MANET. The preceptor based model [12] makes use of training data which has to be collected from past experience and also the cluster head concept where the head monitors for abnormal behavior. Here it is difficult to have clear line of segmentation between the normal and abnormal behavior as it keeps on changing over time.

The behavior based detection [13] defines a profile for the normal behavior and policies which the nodes have to adhere for normal working. Any deviation from the normal statistics is considered to be malicious attempt. It have high false positive rate since no clear line of demarcation.

4. Proposed ANP Flooding attack Detection Mechanism

The proposed ANP-adaptive node profile based detection mechanism for flooding attack in MANET aims at detecting the malicious node and isolating it to enhance the network performance. The node profile based approach has three phases Initialization, detection and isolation phase.

Notations used in ANP approach:

RREQ: Route request packet
PT: Profile table
TS: Timestamp for receiving RREQ

1. Initialization

In profile initialization phase all the nodes in the network build a table called PT and store their profile details. Each node stores all the one hop neighbors profile details. This PT is protected from accessed by the node itself or by the malicious node. The threshold values for RREQ sending and receiving is stored in profile value along with the node identity (NodeId). The threshold value dynamically changes based on the average RREQ flow in the network and the number of users on the network. In [11] the constraints cannot be varied dynamically where as in ANP approach the profile values are varied dynamically and the responsibility of monitoring the threshold value is given to all its one hop neighbor nodes.

2. Detection

In this phase each node upon receiving the RREQ packet will check for its profile and records the TS which will help in monitoring the one hop neighbor activity. Any deviation from the profile value is treated as malicious behavior and the node id is added to the isolation list. Further packets from the source are dropped in order to avoid flooding the network, compared to previous approach[12,13] where the detection do not have clear line of segmentation. The proposed ANP distinguishes the attack traffic behavior efficiently as the profile is made adaptive based on network behavior.

IJERT
IJERT

3. Isolation

Once the detection is confirmed, the malicious node id is taken from the isolation list and broadcasted to the neighbors. The neighbor nodes will further restrict receiving the packets from the malicious node. If the entire one hop neighbor nodes refuse to cooperate for forwarding the packets sent by malicious node, then it cannot communicate with other nodes in the network. The node has been isolated from the network in practice even if it is still on the networks in location. The detection mechanism is run at every node. Each node performs the detection and isolation upon the receiving the route request.

The related scheme [9] only excludes the malicious node from forwarding the packets whereas the proposed ANP approach isolates it from acting as a source to flood the request packets. This approach also removes the malicious node from path i.e. remove its entry from routing table. Still there is possibility that isolated malicious node can send the RREQ to its one hop neighbor and consume their resource like bandwidth at one hop neighbor level. However further flooding and resource consumption at the destination level is prevented.

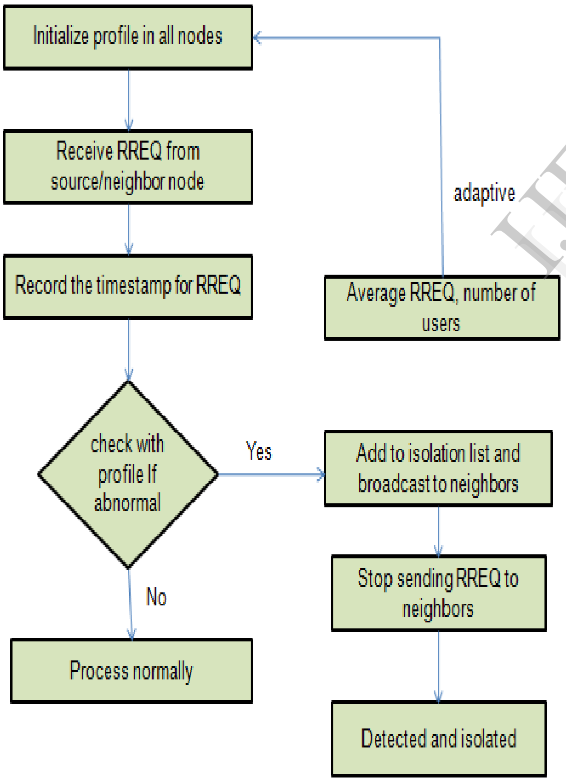

Initialize profile in all nodes
Receive RREQ from source/neighbor node
Record the timestamp for RREQ
check with profile If abnormal
Yes
No
Process normally
Add to isolation list and broadcast to neighbors
Stop sending RREQ to neighbors
Detected and isolated
Average RREQ, number of users
adaptive

Figure 1 Overview of proposed ANP detection mechanism.

IJERT

In this ANP approach, the load imposed by fake RREQ is eliminated by the profile threshold value. The resource consumption like bandwidth is much reduced as described in section 5. The malicious node generating fake RREQ is isolated from the network and hence overhead in node processing time is reduced.

5. Simulation Study

5.1 Simulation environment

Java network simulator jist/swans [14, 15] are used for the implementation for the proposed node profile based detection mechanism. The simulator is extended with customized code for generating the flooding attack and the detection mechanism. The attack structure is shown in the fig.2 here the attacker node H sends the RREQ targeting the destinations; it sends the RREQ more than the allowed RREQ rate limit .Each neighbor node on receiving the RREQ checks with PT and records the TS. Since it is an abnormal flow, the receiving node broadcasts the node id to its one hop neighbor and thereby isolates the malicious node.

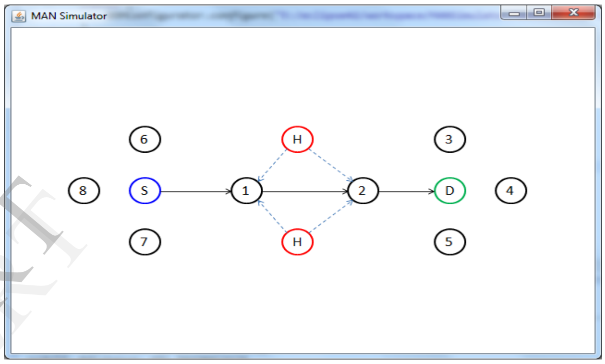


Figure 2 Attack structure for simulation

The profile is initialized based on hello packet interval which is modified for our approach. The PT entry is deleted if the neighbors do not respond with hello packet i.e. if the node moves out of range and no longer act as one hop neighbor. When the malicious behavior is detected, it triggers the hello packet containing the malicious node id to one hop neighbor. This node id is added to isolation list and further RREQ from that node will be discarded by the neighbor nodes. The hello packet interval is modified as per hello interval extension format in RFC 3561.

5.2 Simulation Parameters

Table 1 Parameters used for simulation

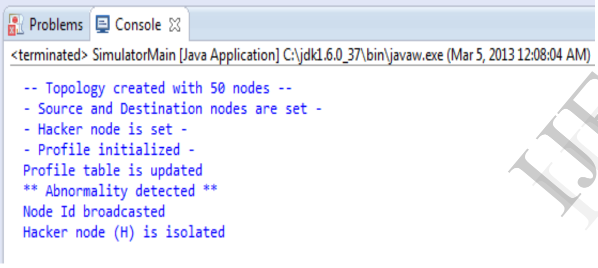
PARAMETER	VALUE
Area	1000 * 1000 m
Simulation Time	50s

Number of nodes	50
Traffic Model	CBR
Mobility model	Random Way Point
Number of attacker	5
Data rate	2Mbps
Packet size	512 bytes

The above simulation parameters are configured in jist/swans. The AODV routing protocol with random way point mobility model and Mac 802.11 is used for study. The scenario of multiple intermediate nodes targeting the same destination is selected for the following simulation study.

5.3 Result Analysis

Profile is set based on the threshold values of the RREQ rate and the number of one hop neighbor nodes. The log file (Fig 3) shows the initialization of profile details and hacker detection. The performance and effectiveness of the detection mechanism is studied in terms of bandwidth consumption, packet delivery ratio and detection rate.



```
<terminated> SimulatorMain [Java Application] C:\jdk1.6.0_37\bin\javaw.exe (Mar 5, 2013 12:08:04 AM)
 -- Topology created with 50 nodes --
 - Source and Destination nodes are set -
 - Hacker node is set -
 - Profile initialized -
Profile table is updated
** Abnormality detected **
Node Id broadcasted
Hacker node (H) is isolated
```

Figure 3 log file showing the detection and isolation

Bandwidth consumption

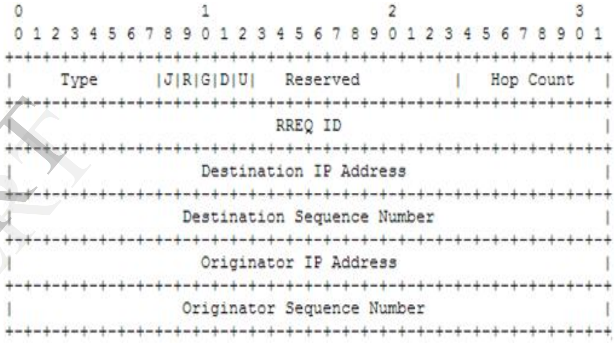
It is measured as the average number of packets received by the intermediate node from source to destination over a period of time and expressed in Mbps.As discussed in section 2; the bandwidth consumption is more due to flooding of RREQ packets. The same has been captured after implementing the profile based detection mechanism. Here there are two cases to be considered.

Case1: Fig.5 shows the bandwidth consumption with flooding attack and proposed detection mechanism. With the proposed ANP detection mechanism the bandwidth consumption due to RREQ is reduced to 60% as it is detecting and isolating the malicious node from clogging the network. Here all the one hop neighbors do not allow the RREQ packets from the malicious node to further flood the victim or the network.

Case2:Fig.6 shows the bandwidth consumption due to RREQ packets at one hop neighbor level i.e. bandwidth consumption at one hop neighbor level of malicious node after isolation phase. The RREQ packet structure as per RFC 3561 is shown in fig.4.Even though the one hop neighbor isolates the malicious node by not forwarding the malicious nodes RREQ packets further into the network, there is possibility that the malicious node can send the RREQ and consume the bandwidth of its one hop neighbor. Here the attacker node H and its one hop neighbor nodes 1 and 2 are considered.

Packet size*No of RREQ packets/Time *10000 -----(1)

The attacker can send the RREQ packets at the rate of 10 to 50 packets to its one hop neighbor. Each attacker can send 10 packets and hence for total of 5 attackers it is 50 packets. The RREQ packet size is 32 bytes. As per (1) the bandwidth consumption ranges from 0.0002560 mbps to 0.0005280 mbps, but this consumption is meager and negligible as the detection mechanism is highly effective in detecting the malicious node.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |J|R|G|D|U|   Reserved          |   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            RREQ ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Originator Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IJERT

Figure 4 AODV RREQ packet format as per RFC 3561

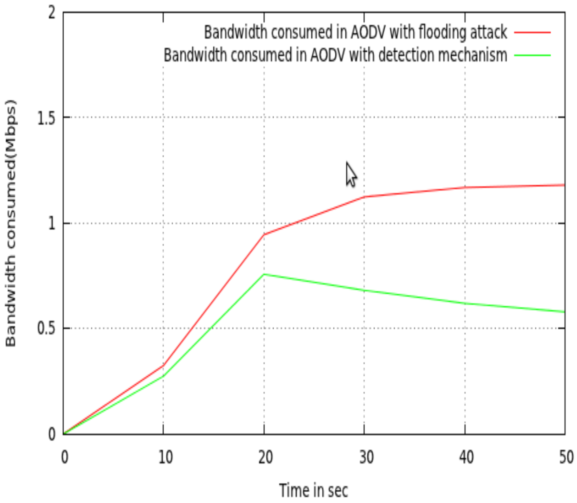


Figure 5 Bandwidth consumption is reduced by 60% with proposed ANP detection mechanism

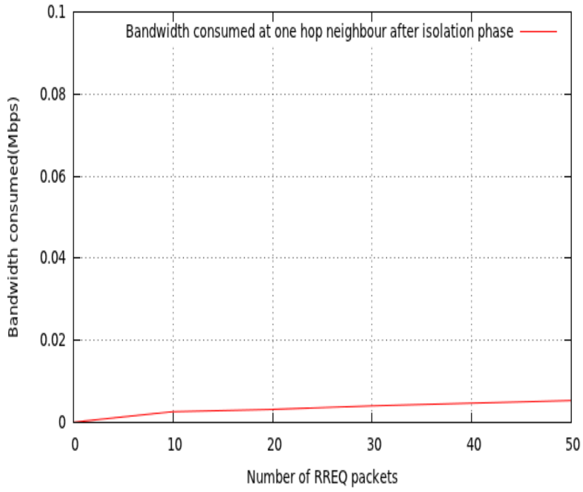


Figure 6 Bandwidth consumed due to RREQ at one hop neighbor after isolation

Packet delivery ratio (PDR)

The packet delivery ratio is the ratio of number of packets received at destination node to that of number of packets sent by the source node. It is expressed in percentage.Fig.7 shows the delivery ratio with flooding attack and proposed ANP detection mechanism.

In case of flooding attack the number of packets reaching the destination is delayed or dropped due to excess RREQ packets in the network targeting the destination. The destination node is busy replying the fake RREQ and hence packets reaching destination is delayed or lost. With the proposed ANP detection mechanism the PDR again raises to 30% once the malicious node is eliminated.

IJERT

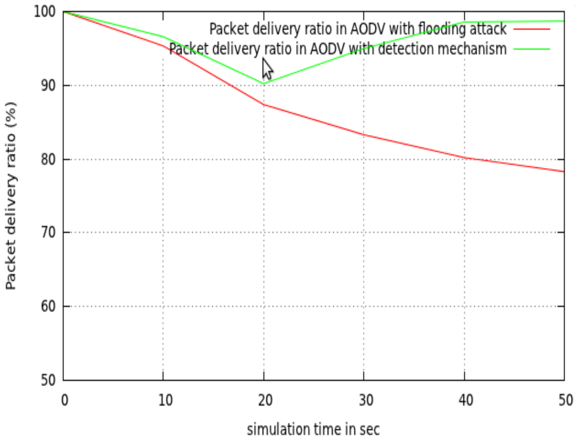


Figure 7 PDR is high after detecting the attacker

Memory overhead

Each node has the profile table that stores the threshold values. Each value occupies 2 bytes so totally each entry in the table occupies 2*3=6 bytes. If there are N neighboring nodes then maximum N*6 bytes is required to store the values. In case if all the 49 nodes are in the radio range then the maximum memory occupied in each node is 49*6 = 294 bytes.

Detection rate

The effectiveness of the proposed detection mechanism is studied in terms of the rate at which the malicious behavior is identified by the participating nodes. The detection rate is defined as the percentage of number of malicious node identified to number of nodes participating in the network. Here the profile is made adaptive and hence the abnormality is detected as and when it starts its behavior.

It also identifies the attackers who impose less attack traffic by cooperating with other attackers. This approach is also effective in detecting the diluted abnormal traffic targeting the network as a whole. Fig.8 shows the detection rate is more in case of increase in number of attackers as it considers both diluted and concentrated traffic targeting the victim or network. In spite of memory overhead being 294 bytes the detection rate shows 90% increase with the increase in number of attacker. This is because with increase in number of attacker the overall attacker traffic flow in the network is increased and hence the attacker is detected efficiently. Initially when one attacker is there the detection rate is only 80% because of diluted traffic and overall attack traffic intensity is less but the detection rate increase over the simulation time as the percentage of attack traffic is increased in overall traffic flow in network.

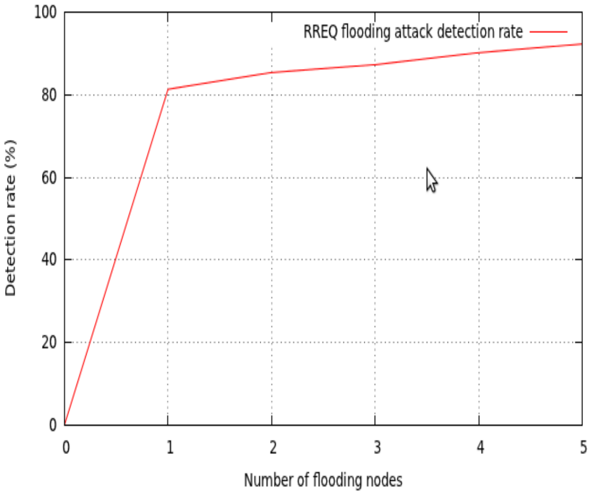


Figure 8 Detection rate for flooding attack

False Positive rate

The false positive rate refers to the situation where one or more node is not malicious but is wrongly identified as malicious because of its abnormal behavior**.** It is calculated as percentage of number of genuine node which is falsely identified as malicious flooding node to that of the total number of nodes in the network.

The FPR can be explained by two cases: In case 1 we say that all nodes can detect the flooding attack but in reality it difficult for all nodes to detect the attacker at same time. There will be situations where some nodes detect the attacker prior to other nodes. The nodes that have not detected the attack will unconsciously forward the bogus RREQ packets to other nodes and it will be wrongly identified as malicious node.

In case II it can happen that normal nodes exhibit abnormal behavior at some point of time.ie the normal nodes under communication process can send RREQ packets frequently to seek routes as the communication routes are broken frequently due to high mobility in MANET[15]. Here also the normal nodes are detected as malicious nodes. As shown in fig.9 the FPR is high in middle of simulation time because of the above two cases. It ranges from 0.019% to 0.023% in middle of simulation time due to higher attack traffic and high mobility. In the middle of the simulation period from 20 to 30 seconds interval there is possibility for wrong identification of malicious node due to the above mentioned behavior.

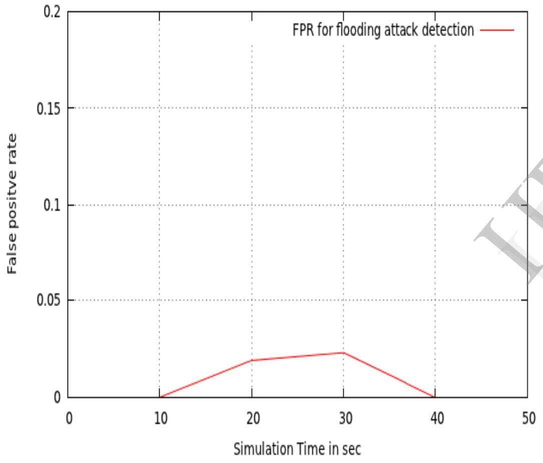


Figure 9 False positive rate for detection mechanism

6. Conclusion and Future work

In this paper, adaptive node profile based approach to detect flooding attack on MANET is simulated and the same has been studied with respect to resource utilization like bandwidth. The proposed ANP detection mechanism is effective in detecting the malicious behaviors at early stage with much less overhead. In future the traffic pattern for the abnormal flow will be studied in detail and the same would be incorporated to the profile for more accurate detection in case of diluted traffic intensity.

References

[1] Imrich Chlamtac, Marco conti, Jennifer J, N.Liu, *Mobile ad hoc networking imperatives and challenges*. Ad hoc networks I (2003) pages 13-64,Elseiver publications.

[2] C.E Perkins, E.M Royer, “*The Ad-hoc on-demand distance vector protocol (AODV)*”, in Ad-hoc networking,C.E.Perkins (Ed), pp 173-219, Addison- Wesley, 2001.

[3] R.H. Khokhar, Md. A.Ngadi, S. Manda. “*A Review of Current Routing Attacks in Mobile Ad Hoc Networks*”, International Journal of Computer Science and Security, 2 (3), pp. 18-29, 2008.

[4] P.Ning,K.Sun,”*How to Misuse AODV:A Case Study of Insider Attacks against Mobile Ad hoc Routing Protocols”*,Proceedings of the 4th Annual IEEE Information Assurance Workshop,60(2003).

[5] ZhiAng EU and Winston Khoon Guan SEAH, “*Mitigating Route Request Flooding Attacks in Mobile Ad hoc Networks*”, Proceedings of International Conferences on Information networking (ICOIN-2006),Sendai,Japan, 2006.

[6] Lee K. Thong. “*Performance Analysis of Mobile Adhoc Network Routing Protocols*”. Thesis Paper submitted to the Department of Computer Science, Naval Post Graduate School, Monterey, CA, 2004.

[7] Bhuvaneshwari K, A. Francis Saviour Devaraj, “*Examination of impact of flooding attack on MANET and to accentuate on Performance degradation*”, International Journal of Advanced Networking and Applications, ISSN 0975-0290 Volume: 04 Issue: 04 pp. 1652-1656, 2013

[8] X. Jin, et al, "*ZSBT: A novel algorithm for tracing DOS attackers in MANETs*," EURASIP Journal on Wireless Communications and Networking, vol.2006, pp.1-9, 2006.

[9] Samesh R. Zakhary and Milena Randenkovic,”*Reputation based security protocol for MANETs in highly mobile disconnection – prone environments”*,International conference on Wireless On-demand Network Systems and Services(WONS),pp.161-167,Feb.2010.

[10] Y. Yoo, S. Ahn, and D. P. Agrawal, "*A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks*," in *IEEE International Conference on Communications (ICC)*. vol.5, 2005, pp. 3005-3009

[11] S. Kannan, T. Maragatham, S. Karthik and V.P. Arunachalam; “*A Study of Attacks, Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols”*; International Business Management, 2011.

IJERT

[12] Y.-A. Huang and W. Lee, "*A cooperative intrusion detection system for ad hoc networks*," In the Proc. Of 1st ACM Workshop on Ad hoc and Sensor Networks,pp. 135-147, 2003.

[13] Neeraj Sharma, B.L. Raina, Prabha Rani et. al "*Attack Prevention Methods For DDOS Attacks In MANETS*" AJCSIT 1.1 (2011) pp. 18-21.

[14] Java simulator for MANET -Jist/swans http://jist.ece.cornell.edu/

[15] R. Barr, Z. Haas, and R. van Renesse. JiST: *An efficient approach to simulation using virtual machines*. Software practice & experience, 35(6):539

IJERT