PDS- A Profile based Detection Scheme for flooding attack in AODV based MANET

Bhuvaneshwari .k[1], Dr. A. Francis Saviour Devaraj [2]

[1]Scholar, Department of Information Science Engineering
Oxford College of Engineering, Bangalore, India
bhuvana.karthikeyan@gmail.com
[2]Professor, Department of Information Science Engineering
Oxford College of Engineering, Bangalore, India
saviodev@gmail.com

Abstract

One of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Flooding attack launched at network layer is a serious routing attack which can consume more resources like bandwidth, battery power, etc. It is more concealed form of Denial of service attack and resource consumption attack. The route discovery scheme in reactive routing protocols like Adhoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) used in MANET makes it more easy for malicious nodes to launch connection request floods by flooding the route request packets (RREQ) on the network. A novel detection technique based on dynamic profile with traffic pattern analysis (PDS) is proposed. Its effectiveness in detecting and isolating the malicious node that floods the route request packets is evaluated using java simulator jist/swans.

Keywords

MANET, AODV, Flooding attack, RREQ, PDS

1.INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are formed dynamically by an autonomous system of nodes that are connected via wireless links without using the existing network infrastructure [1]. The nodes in an ad hoc network can communicate with any other node that resides within its transmission range. For communicating beyond its transmission range, the nodes use intermediate nodes to reach destination [2].

The principal objective of a routing protocol is efficient discovery and establishment of a route between the source and the destination so that there can be a timely and efficient delivery of information between them. The reactive routing protocol AODV [3] invoke route discovery on demand. In other words only when node needs to send information to its peers the route is discovered by the protocol. It does not require the nodes to maintain routes that are not actively used for communication.

1.1 FLOODING ATTACK

The Flooding attack [4] is launched at the network layer by the malicious node. It sends massive amount of control packets to the network. This attack aims at depleting the network resources like

DOI : 10.5121/ijsptm.2013.2302

bandwidth, battery power and thereby preventing the network from providing services to legitimate users. The flooding attack can target the victim node or the network as a whole.

In case of RREQ flooding attack the malicious node imitates like normal node in all aspects, except in performing unnecessary route discoveries. These malicious nodes frequently initiate route discovery to destinations with the intent to flood the network with route request packets. As it is difficult to distinguish between a route discovery initiated with a malicious intent and a legitimate route discovery for repairing broken/stale routes, this type of attack is hard to detect.

1.2 FLOODING ATTACK IN AODV BASED MANET

AODV is particularly vulnerable to RREQ flooding attack because of its route discovery scheme and broadcast mechanism. In AODV the RREQ broadcast is limited by the rate_limit parameter. This rate_limit parameter is self configurable and hence the malicious node would exploit this behavior and start flooding the network with RREQ packets [5]. Each RREQ is associated with unique ‘id’ to prevent redundant broadcast. The malicious node would flood the network with RREQ packets having diff rent’ id’ so that it always appears to be fresh request to other nodes and is repeatedly re broadcasted by them.

The network resource like bandwidth is adversely affected by Flooding attack launched in AODV based MANET. The same is studied through simulation results in Examination of Impact of Flooding attack on MANET and to accentuate on Performance degradation [6] depicting the importance of detection of Flooding attack in MANET.

In the proposed PDS approach, each node is set with profile based on the traffic pattern. Here all the nodes in the network run the detection mechanism to encounter the disseminated attack. The malicious node is detected and isolated by all its one hop neighbors. The evident contribution made by this approach is that it is able to detect the attacker as soon as the attacker starts exhibiting its attack behavior irrespective of the rate limit and unique ‘id’ characteristics.

This paper is organized as follows: Section 2 presents the related work done to detect and prevent the flooding attack in MANET. Section 3 explains the detection features and attack scenario Section 4 describes about the proposed PDS approach and its architecture Section 5 describes the attack model used for study, simulation study of proposed detection scheme (PDS) and its result analysis. Section 6 explains the conclusion and future work.

2. RELATED WORK

2.1 RATE LIMIT BASED APPROACH

The rate limit based [7] approach aims at detecting the route request flooding attack based on certain threshold. Every node in the network is set to adhere to the threshold limit on sending

RREQ packets. However it does not hold good for dynamic environment like MANET. The static threshold values are not sufficient enough to detect the attacker.

2.2 TRUST AND REPUTATION BASED APPROACH

Trust [8] and reputation [9] based schemes are used for identifying the attacker inside the network. Here the genuine nodes which turn to be malicious nodes are considered as inside attacker. The trust and reputation value is set as high and low based on how they co-operatively participate in the

network. Here the false positive rate is high as genuine nodes can also have their value estimated as low on certain scenarios.

2.3 BEHAVIOR BASED APPROACH

The behavior based detection [10] defines a profile for the normal behavior of nodes. Any deviation from the normal profile is considered to be malicious attempt. However the profile is collected one time from the training data and is highly static which does not hold good for dynamic scenarios.

2.4 TRACE BACK SCHEME

In Trace back Mechanism [11] each packet is traced to its source with help of special devices monitoring the network. When these special devices are levied on nodes in the network, the nodes resource consumption will be more. Further centralized equipment is not feasible in the network.

2.5 PRECEPTOR BASED APPROACH

The preceptor model [12] is entirely based on training data collected from past experiences. This model can be applied for only linearly separable data points. The attack instances and the normal instances are linearly separable in the space of detection metrics. This model is effective only when high attack rate is present as the data's can be easily separable in detection metrics and hence easily classified in the perception model.

3. DETECTION FEATURE SELECTION

3.1 ATTACK SCENARIO

The attackers usually use any one of these following scenario [13] for generating the attack traffic. In scenario1, the attacker will send excess amount of route request packets to the destination without adhering to the rate_limit parameter. In this case many RREQ packets with identical (SA, DA) pair will be present in the network. In scenario2, the attackers will attack from different origin with fewer amounts of RREQ packets by adhering to rate_limit. Here many new RREQ packets with different (SA, DA) pair will be present. This case is highly difficult to detect as the attack is originating from different nodes. Further it is also difficult to identify this type of attack packets from that of normal one which is send by genuine node because of link break or stale route.

3.2. FEATURE SELECTION

Two detection features based on the above flooding attack scenario 1 and 2 are designed. The model is described as follows. (N, R, L) where N is the number of malicious nodes, R is rate at which bogus RREQ packets are generated by the malicious nodes; L is the frequency to generate the bogus RREQ packets. The attackers smartly choose these parameters and make it difficult to differentiate attack traffic from normal traffic.

The Detection Feature (DF1) aims at detecting the attack based on the identical pattern of RREQ flows. Here it observes the RREQ packet flow from the same (SA, DA) pair for the sampling interval time T. The flow will be more as the attacker do not adhere to rate limit. This DF1 is enabled based on the rate limit parameter, further the threshold on rate limit is made dynamic based on average number on nodes on the network. The sampling interval is the time difference between any two successive RREQ flows from the same (SA, DA) pair

The Detection Feature (DF2) targets the attacks which are from different origin. Here it observes the new RREQ flows for the interval T. The attacker uses different (SA, DA) pair to launch the attack and they strictly adhere to rate limit. Hence the RREQ flows will be less but new to the receiving node. In this feature the pattern is identified based on unique RREQ' id' for the interval T.The interval T is combination of the path discovery time and net traversal time. The interval T is decided using the below mentioned formula.

Path discovery time= 2*Net traversal time [14] ---------- (1)

4. PDS –DETECTION SCHEME

4.1 THREAT MODEL

In PDS, the Flooding attack is launched by modifying the rate limit parameter for the malicious nodes. The threat model with 50 nodes used for simulation is shown in Figure1. Here there are five attackers each targeting one connection. First category of attackers (H1, H2) is made to send more bogus RREQ without adhering to rate limit i.e. more than 10 RREQ/sec. Second category attackers (H3,H4) is made to send less than 10 RREQ/sec but it is originated from different origin i.e. two source targeting same destination with each 5RREQ/sec. The third category attacker (H5) is made to exhibit both behaviors i.e. for initial simulation time period it sends more RREQ and after certain time it adheres to rate limit (exhibiting second category) but shows malicious behavior.

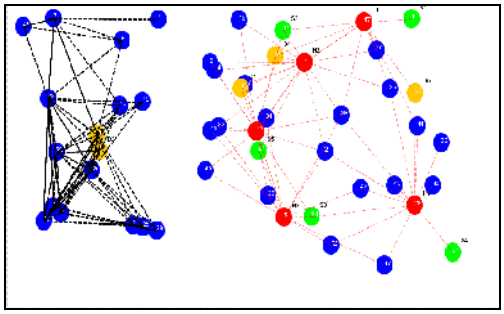

Figure 1.Threat Model

4.2 PDS APPROACH

The proposed detection scheme (PDS) aims at detecting the flooding attack on MANET. The PDS approach uses dynamic profile based traffic analysis to detect misbehaving nodes and isolate them. The PDS approach has two phases of operations detection phase and isolation phase. The PDS system architecture is shown in Figure 2 will have set of modules which try to quantify the normal behavior of the nodes and identify the abnormal behavior of the malicious node. **Normal mode:** This mode collects the details about the normal operation of AODV like sending request receiving reply and data transfer. Here the RREQ broadcast mechanism adheres to the rate limit parameter in sending the RREQ packets. All the nodes will be sending 10RREQ/sec as per RFC3561 [14]. The details in terms of network parameters are collected by the performance mode.

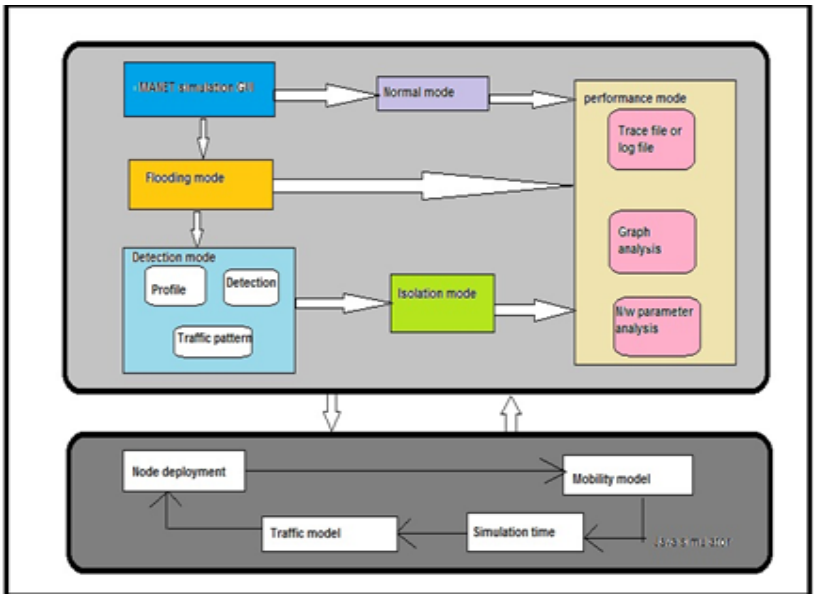

Figure 2. System Architecture

Flooding mode: The attacker is active in this mode. Few nodes on the network are made malicious while other nodes operate in normal AODV mode. The malicious node starts sending bogus RREQ packets without adhering to the rate limit parameter. As the malicious node starts sending the packets there will be degrade in the normal functioning of the network.

The RREQ generator () function is made iterative inside the timer function () in order to generate the bogus RREQ for H1 and H2.In case of H3 and H4 the rate limit of RREQ is kept constant but the frequency is adjusted using the Time interval () function.H5 is made to run all the three function one buy one hence they could exhibit both the attack behavior.

Detection mode: This mode aims at detecting the malicious node which sends the bogus RREQ packets. The threshold value based on rate limit parameter is stored in profile table of each node. Each nodes profile table stores all its one hop neighbor profile information. The profile information is dynamically updated based on the average number of nodes in the network with the help of hello message [15]. This profile table helps in detecting the attackers who exhibit the scenario1 behavior as discussed in section3.1.The next step is to detect the distributed attacker who exhibits the scenario 2 behavior by analyzing the traffic .Detection of attackers adhering to the rate limit parameter is done based on the frequency of RREQ' id' update. The pattern of RREQ 'id' update interval is captured for the sampling interval which is again based on path discovery time. The frequency and pattern of RREQ' id' update helps in detecting the attack from different origin.

Each receiving node would check with its profile table before forwarding the RREQ to its neighbor. The malicious behavior of H1 and H2 would easily identified by its one hop neighbor as the bogus RREQ received from H1 and H2 them will exceed the threshold in profile table. Further the profile table is updated dynamically based on hello message. It is assumed that the profile table is password protected and it cannot be accessed by attackers. The threshold values are dynamic enough to detect the attacker as soon as possible.

In case of H3 and H4 the RREQ 'id' buffered in each of its one hop neighbor will be frequently updated. The time interval of update will be very less in case of this type of attackers. In case of

genuine node behavior each node will be buffering the RREQ 'id and source address for path discovery time. Within this time interval if it receives the same' id' then it discards the packet. For every new set of RREQ there will be unique 'id' generated and new set or RREQ can be originated only if the path is not received within net traversal time. From the above behavior, the interval threshold for the RREQ 'id' update is set and if the nodes exceed the threshold they are classified as attackers. The attacker H5 will be detected in both the cases for its change in behavior.

Isolation mode: The attackers detected in the previous mode should be isolated from participating in the network. If attackers are not isolated they would continue their behavior and thereby deplete the resources and bring down the network performance. The detected attackers are made passive (sending and receiving radio interface are made down) so that they cannot actively participate on the network. Unlike other path cut off process [16] where attacker are added to blacklist and not completed isolated.

Performance mode: The network parameters are captured for the normal AODV operation, flooding operation and detection mode. The performance of the same is analyzed in order to known the effect of the flooding attack and effectiveness of the proposed PDS detection scheme.

5. SIMULATION STUDY

5.1 SIMULATION ENVIRONMENT

Java network simulator jist/swans [17, 18] are used for the implementation for the proposed PDS approach. The simulator is further customized with code for generating the flooding attack and the detection mechanism. The AODV routing protocol with 50 nodes, random way point mobility model [19] is used. The Mac 802.11 protocol is used. The simulation parameter is shown in table1.

Table.1 Parameters used for simulation

PARAMETER	VALUE
Area	1000 * 1000 m
Simulation Time	50s
Number of nodes	50
Number of connection	5
Traffic Model	CBR
Mobility model	Random Way Point
Transmission range	250m
Number of attacker	5
Data rate	2Mbps
Packet size	512 bytes

5.2 RESULT ANALYSIS

The snapshot showing the attack detection and isolation is shown in Figure 3. The effectiveness of the proposed PDS approach is studied in terms of bandwidth, packet delivery ratio, end to end delay and packet drop is discussed in detail below.

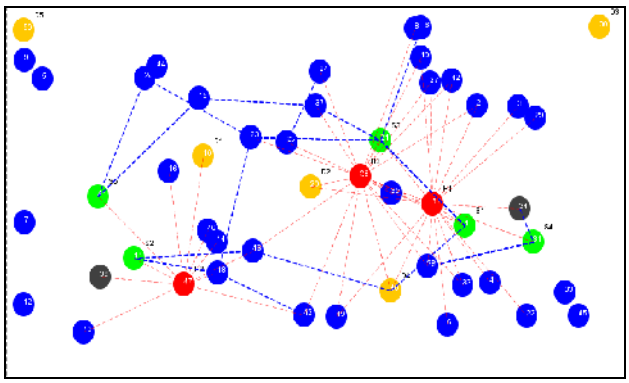

Figure 3. Detection and Isolation (Grey nodes)

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. Figure.4 shows the bandwidth consumption drastically increases throughout the simulation time as the attacker (5 attackers) send out more RREQ packets into the network. By launching the PDS detection scheme the bandwidth consumption is reduced by 54% as it is detecting and isolating the attacker which is clogging the network with bogus RREQ packets. Table 2 shows the percentage reduction in bandwidth consumption with the proposed PDS approach.

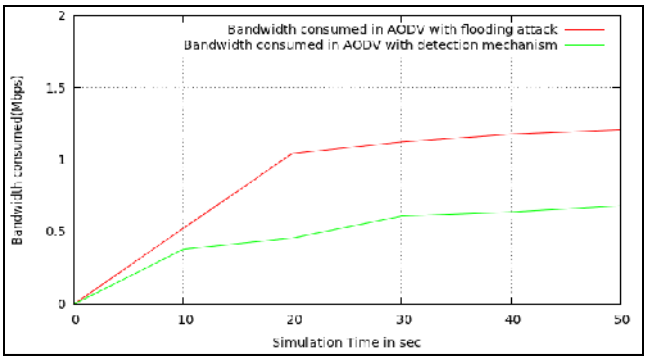

Figure 4. Bandwidth consumption comparison

Table.2 Bandwidth consumption in Mbps

Simulation Time in sec	In Flooding infected AODV	In AODV with PDS	% reduction in bandwidth consumption
10	0.52499671	0.37969132	15%
20	1.04535121	0.58796673	46%
30	1.12453827	0.61022193	51%
40	1.17917472	0.63919989	53.1%
50	1.21107074	0.68091209	54.7%

End to end delay

It is the total time taken for the packet to reach from source to destination and it is measured in seconds. Figure 5 shows the delay with flooding attack is more as the RREQ packets capture the intermediate nodes, so the time taken by genuine packets to reach the destination is more [20]. With the launch of PDS, the delay is reduced by 2.3% as the attacker is detected and isolated from participating in the network. Table 3 shows the decrease in delay with PDS detection scheme.

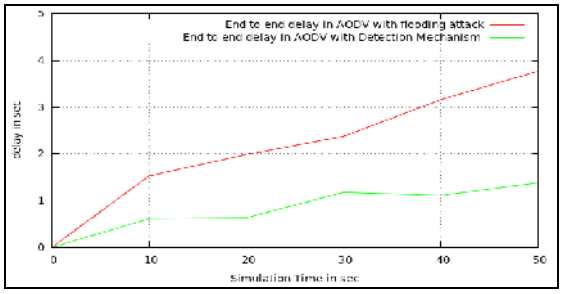

Figure 5. Delay comparison

Table.3 End to end delay in sec

Simulation time in sec	In Flooding infected AODV	In AODV with PDS	% decrease in delay
10	1.529582	0.612438	0.9%
20	1.985656	0.630922	1.2%
30	2.575555	1.197620	1.38%
40	3.161111	1.211664	1.9%
50	3.773232	1.382199	2.3%

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. Figure 6 shows the delivery ratio decreases to 68% with flooding attack. With the proposed PDS approach the PDR again raises to 27% once the malicious node is detected and isolated. Table 4 shows the percentage increase in PDR by launching PDS detection scheme.

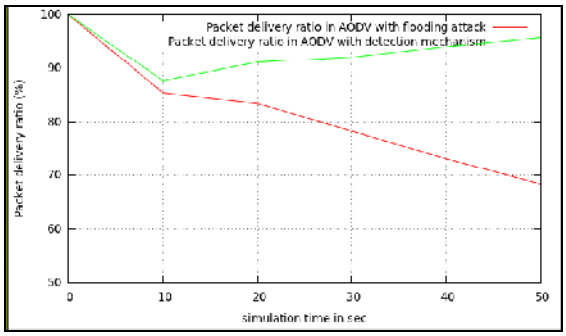

Figure 6. Packet Delivery Ratio Comparison

Table.4 Packet delivery ratio in Percentage

Simulation time in sec	In Flooding infected AODV	In AODV with PDS	% increase in PDR
10	85.320715	87.579390	2%
20	83.381703	91.073361	8%
30	78.281703	91.993356	13%
40	73.181803	93.979390	20%
50	68.281703	95.698340	27%

Packet drop rate

Packet Drop rate is the ratio of number of packets dropped during transmission to that of number of packets sent by the source node.Figure 7 shows the drop rate with floodign attack and PDS detection scheme.The drop is more in case of flooding attack as more of RREQ capture the channel and the destination node busy in processing the bogus RREQ so the packest buffered in destination are dropped as the buffer interval[21] is over.By launching PDS mechanism the drop rate is recued by 25% as the attacker is isolated from the network.Table 5 shows the drecease in packet drop rate.

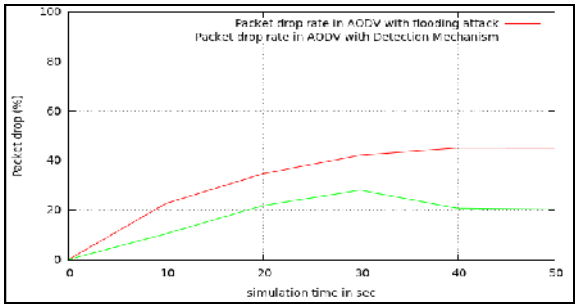

Figure 7. Packet drop rate comparison

Table 5. Packet drop rate in (%)

Simulation time in sec	In Flooding infected AODV	In AODV with PDS	% decrease in drop rate
10	22.618297	10.420610	12%
20	34.679285	21.788644	17%
30	42.133193	28.026639	20%
40	45.158780	20.748686	25%
50	45.119999	20.343434	25%

Response Time

PDS response time is when all the 5 Flooding nodes are detected and isolated from the network. Figure 8 shows the response time of the proposed PDS approach. Here the entire 5 attacker are isolated at different timings. The last attacker (5^{th}) is isolated at 17.4 second after which the network is brought back to stable condition.

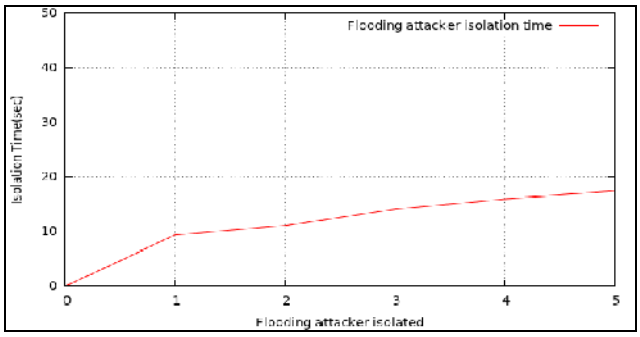

Figure 8.Response time of proposed PDS

PDS Performance Level

It describes the performance of the proposed PDS approach with different attack intensity. The network parameters discussed above are analysed at each level of attackers (1 to 5).PDS response time taken for each attacker and their effectiveness till the response time is discussed below.

Table 6. Performance interference table

Flooding attacker	PDS response time	Bandwidth consumption %	PDR difference %	Drop rate difference %	Delay difference in sec
1	9.34	59%	55%	51%	1.87
2	11.07	47%	43%	44%	1.51
3	14.12	33%	36%	31%	1.33
4	15.97	21%	23%	20%	1.02
5	17.41	28 %	27%	25%	0.93

It is observed from Table 6, that PDS isolates the 1st attacker at 9.34 seconds and completes isolating the entire 5 attacker by end of 17.4 seconds. Bandwidth consumption has come down by 31% at the end on PDS response time. PDR improves by 28% when all the 5 attackers are isolated by PDS during its response time. Packet drop rate improves by 26% from the initial isolation time till the final response time. Average end to end delay has reduced to 0.93 seconds at the end of PDS response time. From the above response time it is clear that the system is able to detect and isolate attacker at faster rate

6. CONCLUSION AND FUTURE WORK

PDS detect the attacker as soon as the attacker starts exhibiting its attack behavior.PDS detects and isolates the attacker efficiently with better response time and do not engage much overhead. In future this work can be further extended for other kind of flooding attacks with respect to AODV like hello packets; data packets etc.PDS can be applied for application involving POS (point of sale) where timely delivery of data is more important in small mobile environment.

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] V.Gupta, S.Krishnamurthy, and M.Faloutsos,”Denial of Service attacks at the MAC Layer in Wireless Ad Hoc Networks”, In Proc.of MILCOM,2002.

[3] 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.

[4] 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.

[5] 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).

[6] 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

[7] 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.

[8] Shishir K. Shandilya, SunitaSahu, “A trust based security scheme for RREQ flooding attack in MANET” International Journal of Computer Applications (0975 – 8887), Volume 5-No.12, August 2010.

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

[11] 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.

[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] YinghuaGuo, StevenGordon, SylviePerreau,”A flow based detection mechanism against flooding attack in mobile ad hoc networks” in proceedings of WCNC 2007.

[14] AODV, http://www.ietf.org/rfc/rfc3561.txt

[15] Bhuvaneshwari .K, A. Francis Saviour Devaraj, “ANP-Adaptive Node Profile based detection mechanism for flooding attack in MANET”, International Journal of Advanced Networking and Applications, ISSN 0975-0290 Volume: 04 Issue: 04, 2013

[16] 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.

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

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

[19] Geetha Jayakumar, Gopinath Ganapathi, “Reference Point Group Mobility and Random Waypoint Models in Performance Evaluation of MANET Routing Protocols”, Journal of Computer Systems, Networks, and Communications, 2008

[20] 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.

[21] YogeshChaba, Yudhvir Singh, Manish Joon, "Simulation Based Performance Analysis of On-Demand Routing Protocols in MANETs,"Second International Conference on Computer Modeling and Simulation, 2010.

Authors Biography

Bhuvaneshwari K is currently perusing her M.Tech in computer networks under VTU University. She has 5 years of software industry experience in Retail and healthcare domain providing ERP solutions. Her research interest includes security issues in MANET, security in Cloud computing.

Dr A Francis Saviour Devaraj has done his B.Sc and M.Sc in Computer Science from St.Xavier's College, M.E (Computer Science & Engineering) from Anna University. He obtained his PhD in computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has also obtained certification in CCNA. He is a life member in technical societies like CSI, ISTE, CRSI, and ISOC. He has around eleven years of teaching experience in leading educational institutions in India and abroad. He has authored/co-authored research papers at the national and international levels. He has atten ded/conducted various national and international level workshops/ seminars/conferences.