International Journal of Scientific Research in Computer Science and Engineering
Vol.6, Issue.3, pp. 1-7 , June (2018)

Research Paper

E-ISSN: 2320-7639

Low Power Distributed MAC Protocol Against Various Kinds Of Attacks By Using Traffic Analysis Methodology

T. Dheepak[1*], S. Neduncheliyan[2]

[1]Dept. of CS, Research & Development Centre, Bharathiar University-Coimbatore, Tamil Nadu, India
[2]Jaya College of Engineering & Technology, Chennai, Tamilnadu, India

Available online at: www.isroset.org

Received: 06/Jun/2018, Revised: 15/Jun/2018, Accepted: 23/Jun/2018, Online: 30/Jun/ 2018

Abstract— The mobile Ad-hoc network (MANET) lacks fixed infrastructure every node communicates with other nodes. The nodes are therefore prevented from crime attack and at the same time the approach called marking on demand is used for the sake of security purpose. The approach called marking on demand is helpful into the MANET for the functions like message sending and data transmission. The MOD (Marking on Demand) Approach is more effective and entirely different from OPM(Opportunistic Piggyback Marking) and MBT (Marking Based Trace back) which have been already existing. The performance of trace back message and message delivery has not been effective. The aim of this paper is to propose the mechanism known as deterministic packet marking for the sake of tracking out the attack which involves in the MANET. The attack , therefore has to be prevented by using MOD and DBT mechanism. The main purpose of the DPM is to investigate and find the solution for the problem of mitigate and counter message. The technical execution is demonstrated through our design with the help of mathematical model, by which the packet delay is reduced. By this approach the packet delivery ratio and the throughput with the energy level are higher in the states of consumption and efficiency.

Keywords— Crime attack**,** Mitigate Counter Message, Traffic analysis, MANET

I. INDRODUCTION

A. Mobile Ad-hoc Network

A Mobile Ad hoc Network (MANET) is a system which organizes itself in the temporary network topologies which are primarily arbitrary by nature. Within this system of MANET, malicious nodes and their attacks have to be detected and removed from the network. Since the MANET is a system of wireless nodes, each node moves independently to any direction but with communicative links within the cluster. The wireless network topology shares the information with other nodes, besides which the manner of exchanging the information is rapid and efficient. The mobile Ad hoc network is a particular variety of ad hoc network which can alter its position and configuration itself. MANET is one of the mobile devices which connect various networks. There are numerous applications which have been implemented into the MANET in the modern era, the MANET contains numerous routing protocols into which they work efficiency.

B. Attack Mitigation

Probabilistic Pipelined Packet Marking (PPPM) is one of the piggybacking methodologies and hence this ppm methodology is identified by the solution and this solution is proposed in this paper. The approaches based on PPM methodology reconstruct the paths which are attacked by malicious nodes the process of transmitting the packets by using the ppm method is more effective than the process of normal transmissions. The source node is the location from where the message are transmitted to the destination In terms of the transmission the data packets are reduced gradually in the source and at the same time the number of data are increased in the destination. Not only the nodes join the network but also leave the network dynamically and also move independently in the MANET. Since the topology is dynamic an adequate physical protection is gained and therefore, the performance of network is enhanced by reducing malicious nodes. Even though the communications are transmitted in a secured manner in the routing protocols, some malicious nodes will disrupt the operational network various attacks occur in the mobile Adhoc networks and those attacks happen both from inside and outside the networks due to the inside and outside attacks the network routing and securing of the data are damaged. Passive attacks is a way of attack in which the transmission of the data is not distributed but the malicious node confirms the route of the transmission from source to destination and manipulate the traffic in order to imitate other authorized nodes. Active attacks is identified by the nature of secure threat to the messages which are prevented in their transmissions from one node to another node. This type of attack paves the way

for unauthorized access to the network and indulges in unwanted functions like modifying packets and therefore congestion occurs in the transmission path.

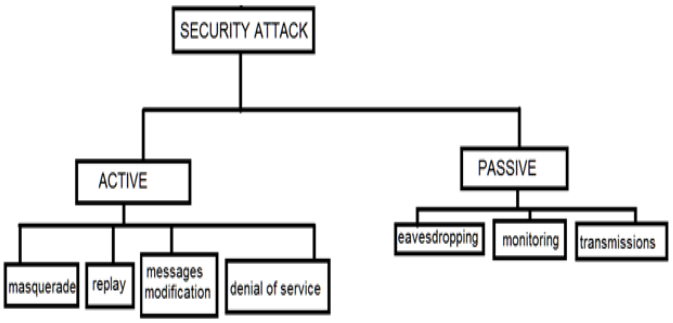

Fig 1.1 Security attacks

C. Crime attack

Crime attacks occur in the medium of message transmission in the network and convert the message into an encoding format and unidentifiable by both source and destination besides which the messages are fragmented by the crime attack and made irretrievable. This type of attack modifies the network path as unidentifiable route and hence it converts the marked packets as unmarked packets When data are transmitted, traffic occurs in the network as the topology changes dynamically and therefore the data are so difficult to be secured in terms the congestion in the network path. The congestion makes an easy way for hackers who discard the packets and therefore the packets become unidentifiable ,We are unable to identify the location of the node because of the congestion.

II. RELATED WORK

Fan Zhang, Wenbo He, Yangyi[1] describes the means of transmission for the sake of sending the data packets in a secured way. A specific method is proposed by the author which is known as FDPM. In this methodology the whole message is split into a number of packets. All the segmented packets are marked by using marking scheme algorithm and then the packets that reach the destination are re modified with the help of reconstruct methodology. The receiving speed of incoming packets is much faster than that of the reconstruction process. The reconstruction process happens in terms of two patterns namely recognition and address recovery. Recognition process is a methodology of decoding. Address recovery is a methodology which marks the data and store in a recovery table.

Mohanapriya Marimuthu and Ilango Krishnamurthi[2] deal with two approachs. The first one is distributed denial of service(DDOS) and the second one is divide and conquer approach. The author proposes three kinds of tasks known as attack tree construction. attack path frequency detection and packet to path association. The proposed scheme presented by the author evaluated the traffic occurs significance in the attack tree construction that is the in band packet marking which is functioning in to the attack tree construction makes sure the repetitive transmission do not occur. The very attack tree construction contains two types of functions called out-band packet marking divide and conquer approach which split up the process and combine again and therefore the result of the process is obtained effectively. In the recent trends, bottom-up approach is preferred to the top-down approach as the latter is controlled by affected nodes. The author proposes a further approach called tree pruning approach which reduces the attack dynamically.

Jerzy Konorski and Szymon Szott [3]identifies the behavior of the nodes whether they are attacked with the help of correlation coefficient parameter. Traffic caused by the real users occurs in the time of transmission. The author therefore proposes the method to distinguish traffic and attack. The attack is categorized into two sections; first one is predictable attack and non-predictable attack. In this type it can be identified the time of interval with the help of enough data of a packet the attack packets are sent to the victim, therefore the behavior of the attack agents become an automatic program me. The program me tries to retransmit the packet transmission repeatedly. In this non-predictable attack, the packet transmission is not allowed to reach other nodes, therefore other nodes are secured with attacks. This method sends the packet in random order, so that the malicious nodes cannot identify the packets.

T Divya Sai Keerthi, Pallapa Venkataram [4] the authors' focus concentrates upon the security attack occur in the mobile ad-hoc network. Security has become a core issue for communication which is secured between mobile nodes in a hostile situation. MANET is something which is easily approachable for both authorized users of network and malicious users of network. In the presence of malicious nodes one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. MANET can operate in isolation or in coordination with a wired infrastructure. The author describes two types of routing attacks such as active and passive attacks. The active (flooding, black hole, spoofing, wormhole) and passive (eavesdropping, traffic monitoring, traffic analyses are described. These analyses have the security threats. An ad hoc network faces the security threats and presets the security objectives. The existing proposals find out the attack that occurs first and then enhances the security levels for the existing protocols.

Hamid Alipour, Youssif B. Al-Nashif, Pratik Satam[5] propose a MANET is an infrastructure-less type network, which consists of number of mobile nodes with wireless

network interfaces in order to make communication among nodes. We discuss various types of attacks on various layers under protocol stack. Different types of attackers attempt different approaches to decrease the network performance and throughput. The principal focus is on routing and security issues associated with mobile ad hoc network which are required in order to provide secured communication. In the network, communication can be classified into two groups: insider and outsider communications. An insider attacker is an authorized node and a part of the routing mechanism on MANETs. These paper discuses different layers under protocol stack that becomes vulnerable to various attacks. The study proposes to use algorithm to prevent different types of attacks.

III. PROBLEM IDENTIFICATION

The proposed scheme that has been existing fails to defect which message is irrelevant and which node acts as an original message and which is to be eliminated from the cluster. Because of this , the previous work could not analyze the alternate path to select the best path. The time slice therefore increases for the packet which is sent from source to destination on the other hand the packet delivery ratio is also decreased. Due to the unwanted network and malicious node the consumption of power is higher in level. The source at the same time, identifies the location of the packet.

A. Proposed Approach

crime attack model: These kinds of attacks come under traffic analysis scheme. The specialty of the scheme is that which sends the duplicate message through the cooperative and homogenous network. The crime attack happens by the traffic that occurs due to the trespass of unauthorized nodes into original nodes and act as original nodes. In this situation , the source node plays an important role. The source node releases the first packet message and monitors continuously until acknowledgement is received from its destination node in order to avoid unauthorized message of malicious nodes from the original message with the help of encryption and decryption. This process continues until all the original message are received from source to destination in the MANET.

B. Traffic Analysis

In this method , when an attack occurs in the network, the unauthorized node is destroyed . Traffic analysis is a process in which any message is intercepted and examined in order to find the relevant message otherwise the unauthorized information is deleted from the patterns of communication. This process can be performed even the message are encrypted. The process traffic analysis is so inevitable to confirm the authenticity of message in the server by manipulating the vulnerability of the system.

C. Path Selectionand Data Transmission

The function of the source node is to transmit the data packet to the destination in which the source selects the path of the data packet dynamically in order to avoid congestion. The source node identifies the best path which is devoid of malicious node by using the mechanism called deterministic packet marking (DPM). In the process of data transmission the neighbor node sends acknowledgement of receiving authorized data packets to the source node. In case of finding unauthorized message from a malicious node the source node immediately changes the path which is devoid of malicious trespass and traffic. In the transmission path traffic occurs unexpectedly due to conglomeration of messages and hence the source node tries to update the undelivered packets. The traffic is changing the path structure to breadth first search tree model. In the MANET network , left child and right child are categorized as sub graph. Message are transmitted as fragmented packets from source to destination in order to avoid traffic

D. Mitigate Counter Message

When the messages are transmitted from source to destination the messages are split into data packets and every packet is assigned a value. When the data packets are being transmitted the value of data packets in the source node is decreased while that of the data packets in the destination is increased. In case of an Imbalance of values between the source and the destination, it covers the idea that the data packets are not transmitted properly. The source node therefore resends the undelivered data packets to the destination.

E. Transmission Design And Fictitious Setting Mechanism

When the data is transmitted from one node to another node protocol 802.11 is applied in its operation in the transmission process. When the destination node cannot receive the message from the source node the host node receives the message and sends it to the destination. This proposed scheme plans the function in which the nodes which send date or messages are found and eliminated from the network and also it makes sure whether the destination node have made any damage in the mechanism. The destination nodes send acknowledgement for receiving data from the source node. In case of an acknowledgement interruption, it can be confirmed that a malicious attack has occurred in the network path. By using this mechanism, nodes are either added or removed. When the nodes are genuine they are accepted and included in the network, otherwise the intruder node will be disseminated.

F. Advance Opportunistic Piggyback Marking

The extension of OPM is AOPM in which the MOD methodology is implemented therefore the AOPM contains fragment of message to be transmitted to the next neighbor node. The messages are stored in buffer before transmitting to the next node due to the reconstruction of the next path. Having reconstructed the network path. The MOD has the

objectivity to transmit the packet of fragmentations through specific flow of traverses. The intermediate node not only captures the fragments of packets but also decides which node is the best neatest node to be sent; the entire process of transmission is carried out within time slice by using trace back performance. When the packets are transmitted from source node to target node, the message are reassembled and organized as original message. The process of transmission of fragmented packets is carried out through TCP header. If the receiver selects the fragment packet it is successful or else it is known as lose of packet. In terms of successful transmission of packets to the target node, the consumption of energy level is distributed to all the participant nodes equally. Therefore the energy level of nodes and the proportion of packet delivery are enhanced and maximized.

G. Preventing the Precursor Attack and Energy Level Maintaining

If an attack is to occur, it has to make use of path initialization and to mitigate counter message instead of analyzing the duration and fragment packet size. Initial node has to select the next node to transmit the packets for which it selects randomly instead of sequential mode. In the process of selection , the initial node selects multiple paths instead of single selection. The source node stays in the network a until the packets are delivered to the target node. Therefore the precursor attack happens very easily because of this state explained previously and hence the nodes are retained in the functional mode. The consumption of energy as a result is in higher level. The primary way to prevent this kind of attack is to change and reform the path and therefore the attacker fails to identify the path of transmission from one node to another node. By this process, energy level is distributed among neighbor nodes equally and maintained properly.

H. Algorithm

A MOD approach enabled to IP packet header and process of received packet on AOPM
Procedure collects the fragment packet
Initialize fragment packet=FP
If
{ selected FP==true then
MOD(FP==true && FR. receive< >R.add then
FP is a MOD and R is not the goal node of FP
G=Generate of packet (P)
FP=fragmentation of (G)
Accumulate (FP. FP.rec)
Else transporter(F.P)== true then
/* check the transmitter node then whether the packet are receive or not
FP=Get fragment selects(P.FP)
Transmitted(FP) }

I. MATHEMATICAL CALCULATION

Tput – Throughput
Ti – complete time consumed by node
Tp- spent time for individual separate packets
Tnp-spend time for neighbor packets
DR- Data rate
k- no of packets
Np-node power
Npp- node power personal packets
Nnp-node power neighbor packets
Ut-total utilization
N Rn- Number of route utilization

P is a packet which is the sum of personal or neighbor packets. For which a node forwards where as $\sum_{i=1}^{n} Pi$ is the sum of a node transmit packets received from one or more neighbors. The variable 'K' is assigned for the total number of transmitted packets.

In the process of transmission, message are transferred as packets in which a single packet is transmitted in the network by using the $\sum_{i=1}^{n} Pi(pi)$

The formule to calculate the total time of transmission is ti=+pp+Tnp

Tput = $\frac{Total \text{ packet forward}}{Total\ time}$

Tput= $\frac{node\ s\ packet+neighbor\ packet}{Total\ time}$

The total of number of packets a node can transmit.

Tput = $\sum_{i=1}^{n}(\text{pi} - \text{ki})$

single packet

ti= $\sum_{1}^{k} tpp(k) \sum_{1}^{n}(K) 1 \leq k < \alpha$

number of packet are bounded between 1 and the infinity.
time required transmit a neighbor nodes.

t = $\frac{\text{number of packet}}{data\ rate}$

major components of the Time division algorithm. It concept of asymmetric division

tnp = $\frac{p(1-k)\text{n}}{DR}$

NP is power of node and k is no of packet that a node can transmit. $U = \frac{Nout}{Nin}$

The consumption of power distribution among packets is not uniform when the utilization numerator and the denominator are unknown.

Nppout=$\sum_{i=1}^{k}(p\ pout - k\ pout)/tpp$

the Npin is relationship between input and output

Npin =Npnin

Npnin = $\sum_{i=1}^{k<\alpha}(\{\text{pnin} - \text{knin/tpp}\})$

the router to interpreted

Ut= UR1+UR2+UR3+……..+URn

Ut = $\sum_{k\geq 1}^{k<\alpha}(\{\text{pnout/tpp}\}) + \text{Kpout/tnp}\})$ The results of compute the packets are send to neighbor node in the original data can be transmit the alternative path. With neighbor node are utilized by all other node

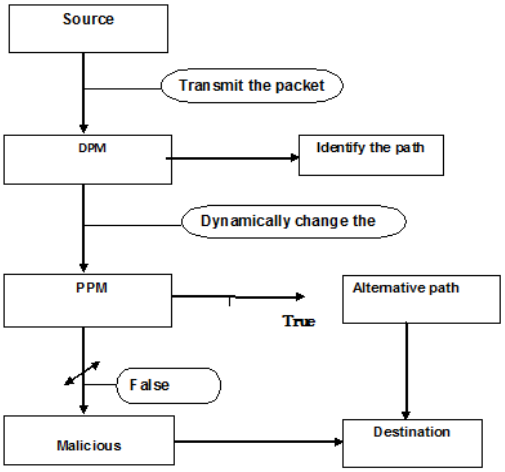

Fig 4.1 System Architecture

IV. RESULT AND DISCUSSIONS

The proposed protocol is compared to the existing protocol by following metrics and as a result the throughput and packet delivery ratio are increased on the other hand the time delay and routing overhead are decreased. The results of simulation by using NS2 obtained from various scenarios show their impacts that the network traffic is mitigated and the energy level of nodes is increased. The proposed scheme calculates the optimal transmission routing and it analyzes the data packet in order to verify the node whether it is authorized in the cluster. In the present methodology, the best neighbor node is found out with alternative path whereas this was not carried out the previously existing scheme.

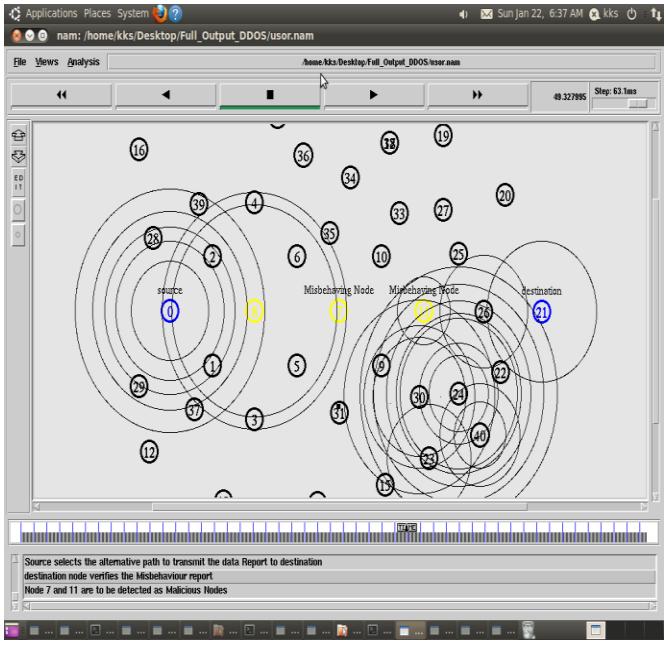

Fig. 4.2 source node identify the malicious node

Figure 4.2 portrays the process of identifying malicious node and also finds out the number of packets sent in a second. It is shows that the process preventing attacks occurring in the transmission.

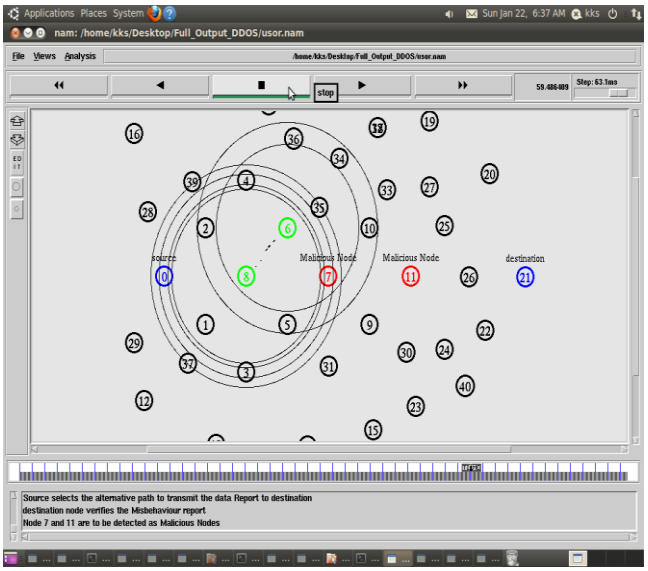

Fig.4.3 the source node select the alternative path

Figure 4.3 portrays the process of selecting the alternative path (ie) number of packets sent in a second when a communication had been made between sender and receiver the figure shows that the proposed approach has reduced 80% of the data transmission.

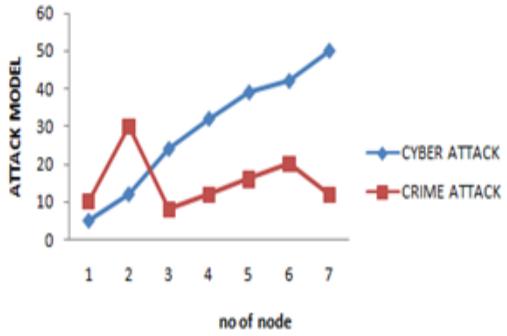

Fig. 4.4 Comparison of two kinds of attacks

This study used ns-2 as the network simulator and conducted various simulations to evaluate the proposed performance of all the nodes are randomly scattered with a uniform distribution. The location of the sink is randomly determined this study that evaluates the routing performance under Comparing packet delivery ratio for existing and proposed scheme.

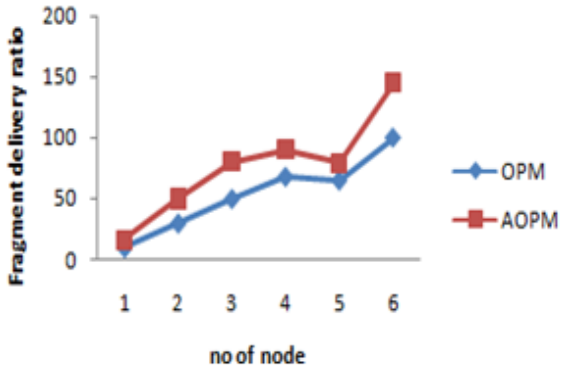

Fig. 4.5 Comparison of OPM and AOPM

The OPM and the AOPM are the two methods which are compared by using fragment delivery ratio. As a result the delivery ratio of the AOPM is 98% to be compared to the delivers ratio of OPM.

V. CONCLUSION

In This paper analyzes the security scheme of the protocol of IEEE 802.11 and also reviews the methods which mitigate counter problem. The core focus of this paper falls mainly on the solution that prevents traffic in the network and attacks that occur in IEEE802.11. The current approach investigates how traffic happens in the network path and how fake message mingles with authorized message, with the help of trust based scheme.

REFERENCES

[1] Fan Zhang, Wenbo He, Yangyi Chen, Zhou Li, XiaoFeng Wang, Shuo Chen, and Xue Liu," Thwarting Wi-Fi Side-Channel Analysis through Traffic Demultiplexing", IEEE Ttransactions on Wireless Communications, vol. 13, no. 1, january 2014.

[2] Mohanapriya Marimuthu and Ilango Krishnamurthi," Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks", journal of Communications and Networks, vol. 15, no. 1, february 2013.

[3] Jerzy Konorski and Szymon Szott," Discouraging Traffic Remapping Attacksin Local Ad Hoc Networks", IEEE Transactions on Wireless Communications, vol. 13, no. 7, July 2014.

[4] Leovigildo Sánchez-Casado, Gabriel Maciá-Fernández and Pedro García-Teodoro," An Efficient Cross-Layer Approach for Malicious Packet Dropping Detection in MANETs", 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[5] Hamid Alipour, Youssif B. Al-Nashif, Pratik Satam, and Salim Hariri, "Wireless Anomaly Detection Based on
IEEE 802.11 Behavior Analysis", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 10, OCTOBER 2015.

[6] Long Cheng, Dinil Mon Divakaran, Wee Yong Lim, Vrizlynn L. L. Thing," Opportunistic Piggyback Marking for IP Traceback", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 2, FEBRUARY 2016.

[7] Prasenjit Choudhury,Subrata Nandi,Anita Pal, Narayan C. Debnath," Mitigating Route Request Flooding Attack in
MANET using Node Reputation, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 2, FEBRUARY 2012.

[8] T Divya Sai Keerthi, Pallapa Venkataram," Locating the Attacker of Wormhole Attack by Using the Honeypot", 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[9] Hamid Alipour, Youssif B. Al-Nashif, Pratik Satam, and Salim Hariri," Wireless Anomaly Detection Based on IEEE 802.11 Behavior Analysis", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 10, OCTOBER 2015.

[10] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007, page, 85-91

[11] Z. Karakehayov, "Using REWARD to Detect Team BlackHole Attacks in Wireless Sensor Networks," Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.

[12] S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[13] S. Kurosawa et al., "Detecting Blackhole Attack on AODVBased Mobile Ad Hoc Networks by Dynamic Learning Method," Proc. Int'l. J. Network Sec., 2006.

[14] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[15] Jyoti Raju and J.J. Garcia-Luna-Aceves, " A comparison of On-Demand and Table-Driven Routing for Ad Hoc Wireless etworks'," in Proceeding of IEEE ICC, June 2000.

[16] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[17] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conf. 2004.

[18] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," Proc. 2002 ACM Wksp. W[12] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[19] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," Proc. 2002 IEEE Int'l. Conf. Network Protocols, Nov. 2002.

[20] C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., 1999.

[21] Y. Xie and S.Z. Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," IEEE/ACM Transactions on Networking, vol. 17, no. 1, pp. 15-25, February 2009.

[22] Y. Chen and K. Hwang, "Spectral Analysis of TCP Flows for Defense against Reduction-of-Quality Attacks," in Proceedings of the 2007 IEEE International Conference on Communications (ICC'07), pp. 1203–1210, June 2007.

[23] F. Yi, S. Yu, W. Zhou, J. Hai and A. Bonti, "Source-Based Filtering Algorithms against DDoS Attacks," International Journal of Database Theory and Applications, vol. 1, no. 1, pp. 9-22, 2008.

[24] S. Yu, T. Thapngam, J. Liu, S. Wei and W. Zhou, "Discriminating DDoS Flows from Flash Crowds Using Information Distance," in Proceedings of the 3rd IEEE International Conference on Network and System Security (NSS'09), 18-21 October 2009.

[25] Y. Chen and K. Hwang, "Collaborative detection and filtering of shrew DDoS attacks using spectral analysis," Journal of Parallel

and Distributed Computing, vol. 66, no. 9, pp. 1137-1151, September 2006.

[26] T. Tuncer and Y. Tatar, "Detection SYN Flooding Attacks Using Fuzzy Logic," in Proceedings of International Conference on Information Security and Assurance (ISA'08), pp. 321-325, 24-26 April 2008.

Authors Profile

Mr.T Dheepak pursed Bachelor of Science from A.V.V.M.Sri Pushpum College, affilated to Bharathidasan University in 2001 and Master of Computer Applications from Periyar mainyammai college of technology for women affilated to Bharathidasan University in 2004 and Master of Engineering in computer science from Pavendar Bharathidasan College of Engineering and Technology, affilated to Anna University in 2006 He is currently pursuing Ph.D. in Bharathiar university and currently working as Assistant Professor in Department of Computer Sciences, Bharathidasan university college at perambalur. He has published more than 3 research papers in reputed international journals and conferences also available online. His main research work focuses on Energy efficiency , security scheme in MANET and He has 9 years of teaching experience and 5 years of Research Experience.

Dr.S. Neduncheliyan pursed B.E. degree in Computer Science & Engineering from the University of Madras in 1989. and M.S.degree Specialized in Robotics Engineering from Universiti Sains Malaysia, Malaysia in 1999 and Ph.D in Faculty of Information and Communication Engineering from Anna University, Chennai in 2009 and He has a total teaching experience of 25 years. He has published 20 research papers in International and National Journals. He has also presented 55 research papers in National and International conferences. He is currently guiding Five students towards the award of Ph.D degree in Anna University. His areas of interest are: Wireless Sensor Networks, Computer Networks, Interval Analysis and Robotics.

