IJCSE International Journal of Computer Sciences and Engineering Open Access
Study Paper Volume-4, Issue-5 E-ISSN: 2347-2693

A Study on Security Threats in Manets

Vaidya Omkar[1], Gautam Amiya[2], N Jaisankar[3*]

[1,2,3*] School of Computing Science and Engineering,
Vellore Institute of Technology, Vellore

Available online at: www.ijcseonline.org

Received: Apr/26/2016 Revised: May/02/2016 Accepted: May/14/2016 Published: May/31/2016

***Abstract*— MANETs have very unique characteristics like dynamic topology, wireless radio medium, limited resources and lack of centralized administration; as a result, they are sensitive to different types of attacks in different layers of protocol stack. Each node in a MANETs is capable of acting as a router. Routing is one of the aspects having various security concerns. MANETs has no rigid line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of mischievous nodes, one of the main challenges in MANETs is to design the robust security solution that can protect MANETs from various routing attacks. This paper present survey of common attacks on network layer namely Black-hole, Wormhole and Gray-hole attack which are serious threats for MANETs. This paper also discusses some proposed solutions which help to detect and prevent these attacks. MANETs can operate in isolation or in coordination with a wired infrastructure, often via a gateway node participating in both networks for traffic relay. This flexibility, along with their self-organizing powers, is one of MANET's biggest strengths, as well as their biggest security weaknesses.**

Keywords- MANETs; Security; Attacks; Wormhole Attack; Black-hole Attack; Gray-hole Attack

I. INTRODUCTION

MANET (Mobile Ad-Hoc Network) [1] is a continuous self-configuring network that consists of mobiles as nodes; hence it is an infrastructure-less network. Any number of nodes can join or exit the network. This makes MANETs *mobility prone*, thereby rendering it to be highly dynamic in nature. A MANET is a most assuring and incrementally growing technology which is depends on a self-organized and rapidly deployed network. Due to its great and user friendly features, MANET easily used in the different real world application areas where the networks and its topology changes very quickly. Nodes in MANETs can attach and detach the network at any time, i.e., dynamically [1]. There is no fixed infrastructure and any centralized administration in this type of networks. Nodes are connected to each other through wireless interface. The dynamic quality of such type networks makes it highly sensitive to various link attacks. The basic requirements for a secured networking are secure protocols which assure the confidentiality, availability, authenticity, integrity of network. Many current security solutions for wired networks are inadequate and inefficient for MANET environment. As the conversation occur in free medium form the MANETs more sensitive to security attacks. In the presence of security protocol effect of various attacks can be decreased. The mobile hosts dynamically establish paths among one another in order to communicate. Therefore, the achievement of MANET communication highly based on the collaboration of the involved mobile nodes.

Every node in MANET has full freedom to follow any path and is so altering its associations always and often. Every node consumes information relevant to it and the remaining information is passed to other nodes. We see here every node is thus acting as a router. The main design issue in MANET is that every node has the necessity to keep up its routing data. It may work autonomously on itself or might be linked to the Internet. It is a collection of one or many various transmitters–receivers among themselves. MANETs work above the Link layer and are made up of one to one, building on its own and getting rid of the defects on its own variety of collection of communicating nodes. Nowadays MANETs talk at the rates of 30 MHz -5 MHz

Types of MANETs

1. **Vehicular Ad-hoc Networks (VANETs)**: Transportation equipments are equipped with MANET's. If they have some non-natural IQ associated with it, they are known as In VANET (Intelligent Vehicular networks) and are useful in minimizing mishaps on roads due to transportation means.
2. **Smart Phone Ad-hoc Networks (SPANs)**: It uses the existing physical components in nodes like Bluetooth and Wi-Fi to create one to one friend to friend to friend associations with no use of conventional mediums of communication. They are not like conventional hub and spoke networks as there is no centralization and use sending of messages at many jumps from one node to the other.

Also any node can abandon the MANET whenever it desires. Without collapsing the network.

3. **Internet based mobile Ad-hoc networks (iMANETs)**: In this type, parts of MANET are associated to a centralized Internet –gateway.
4. **Military/Tactical MANETs:** Used for army to military operations, like, spying on the enemy.

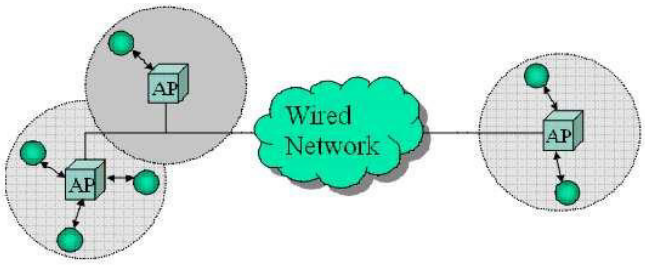

Fig-1: Infrastructure Based Network

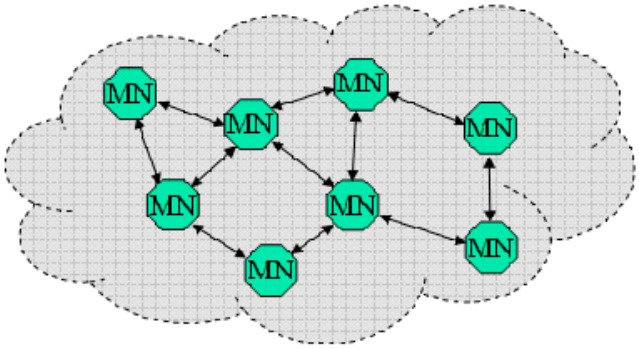

Fig-2: Infrastructure-less Network

Fig-1 represents the network which is totally based on infrastructure. Infrastructure based network consists of wired network and Access Point (AP). Fig-2 represents the network which is infrastructure-less. Infrastructure-less network consists of Mobile Node (MN). Security has become a primary issue in order to provide protected and secured communication between nodes in a wireless network. In a mobile ad hoc network, it is much more vulnerable to attacks than a wired network due to its limited substantial security, volatile network topologies, power-constrained operations, and lack of centralized monitoring and management point.

Merits of MANETs

- It provides access to information and services regardless of any location.
- This type of networks can be set up and deployed at any place and time.
- No any pre-existing infrastructure need to develop this network.

Demerits of MANETs

- Lack of authorization facilities: Intrinsic mutual trust is vulnerable to attacks.
- Limited resources: Limited resource invokes the problem of limited security.
- Time varying topology: Volatile, changing network topology makes it hard to detect malicious nodes.
- Security protocols for wired network cannot work for ad-hoc networks.

II. LITERATURE SURVEY

Many scientific works have been carried out for identifying nodes with the bad intention of damaging MANET in one way or the other. It is discusses as follows:

Wenjia Li, Anupam Joshi, and Tim Finin, developed a new idea of classifying MANET devices with respect to their working or operational attitude. They utilized Support Vector Machine to build faith. They measured the operational attitudes in terms of Pack abandon frequency, Pack Change Frequency, and Pack Misdirected frequency [1].

Bo-Cang Peng and Chiu-Kuo Liang, frames the concept of positive bondage data to disclose the assault on MANETs. This data gathers all the information about positive bonding between MANET devices and its nearby MANET devices. It has broadly two parts-primary key of the nearby nodes and its bondage info place in the system-whether it is positive, negative or neutral in terms of close comrade, distant social contact and stranger. Whenever a pack is collected, this information is accessed. By default, every device will be taken as stranger, if the confidence on it grows it will be taken as distant social contact and if ultimately if the communication with that particular device is successful often, it will be upgraded to close comrade. [2]

Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris, discovered a new way to differentiate between black and gray-hole MANETs. The transmitter tries to assure via all the paths the destination gets all of its expected packs. To avoid a black hole which interferes with the communication, the transmitter pings a pack to verify and validate this thing to all the MANET devices and at the receivers side also the response follows alike path as the transmitted info. [3]

D.M. Shila and T. Anjali invented a way out to the gray-hole attacks in MANETs. First stage is with respect to the direction opposite to the special level at which things begin and uses this special level and pack increment/decrement register or variable to form division of assaults. The second stage is with respect to interrogation and commendation from the in –between devices to stop the assaulter. [4]

X.P. Gao, and W. Chen made collective sign procedure to find and locate pack falling MANET devices. It had basically three integrated components- 1) making evidence procedure. 2) Identification procedure 3) Examination and inspection procedure. [5]

Author Hongmei Deng, Wei Li, and Dharma P. Agrawal made it easy to understand stand-alone black Hole MANET device recognition. This mechanism has all in-between devices return the next-jump data on receiving an RREP note. On receiving the response, the source need not transmit the info, only extract the next –jump data and again transmit request to the next jump to support that it has a course to in –between device which returns the response and it has a way to final receiver device. [6]

Tamilselvan L and Sankaranarayanan V, gave the temporal Special boundary value recognition with respect to the expansion of actual AODV protocol. It has clock established to form the Clock expiry data for gathering the extra call from the devices on receiving leading call. It stores the chronology and receiving time in collect route reply table (CRRT), maintain the sum total timeout data with respect to the ingoing time of first path appeal, and knowing if the path is appropriate or not with respect to the temporal special boundary value. [7]

Payal N Raj and Prashant B Swadas, formed the concept of DPRAODV (discovery, evading and responsive AODV) to anull the protection of black holes by notifying remaining devices in the MANET. It performs usual AODV (a device gets RREP pack verifying chronology through routing table. The special boundary value is refactored in the period. [8]

All the above techniques add to the computation in MANET devices, but as it has finite power supply, it is need to develop rules for MANET that decreases computation in MANET devices. [9]

Hakem Beitollahi, Geert Deconinck does study of steps taken against DDoS (Distributed Denial of Service assaults.They study in detail and compare and scrutinize every of these techniques and give their merits and problems in all of these schemes. If feasible, it develops a protection method from the assaulter's angle of approach. It discusses popular D-DoS protection methodologies fully. With respect to this paper, users can find proper protection methodologies to fight D-DoS assaults and their competency to do so. It has applications and is useful for both the teaching community as well as manufacturing and trading companies. [10]

Ningrinla Marchang a, Raja Datta invented two assault recognition methods in MANET's. It is based on the collective support of nearby devices in MANET to identify a damaging device nearby. One method is used to find damaging devices nearby where any two devices are so close to Trans-receive radio signals. This collection of devices is called clique. Other method has the case where the nearby devices may not be so close, however there is at least a device which is centrally located or close to the other devices. This collection is alike with a cluster. All the two methods apply note dispatching.one device is used to look after the identification of damaging devices. Every device uses the communication for identification to evaluate the harmfulness of devices and throws votes to this looking after device which examines through the votes these doubtful devices to be damaging or not. It does not follow direction-finding rules. First one works whenever there is complete communication. All the two methods have good efficiency and effectiveness. [11]

Sudip Misra a, P. Venkata Krishna , Kiran Isaac Abraham, Navin Sasikumar b, S. Fredun do a survey of effects and consequences of DDoS on WMNs.It is with respect to OLSR(Optimized Link State Routing Protocol) and uses Automata theories and artificial intelligence to prevent DDoS in WMN's. [12]

Hung-Jen Liao , Chun-HungRichardLin ,Ying-ChihLin , Kuang-YuanTung gives a complete analysis and comparison of problems in IDS.A classification is developed for recent IDSs.Diagrams etc. are also given to catch up things in a lucid way. [13]

Shelly Xiaonan Wu, Wolfgang Banzhaf do study of various CI approaches to the IDS problem-defintion.The works are briefed at the end and the present problem scenario and future works are also defined. [14]

Adrian P. Lauf, Richard A. Peters, William H. Robinson study the formation of two-phase IDS for MANET's.They try to find out the background of the dealings and map it to a function. In initial phase, they deploy global and local maxima in PDF of their conduct and manners. This gives the distinctive conduct and manners as the output of this phase. In the final phase, it does cross-verification and identification of assaults concurrently. The total effect is to find damaging devices in a gradable fashion and work well also when 22% of devices are damaging. [15]

III. METHODOLOGY

Assaults in MANETs-

Assaults in Mobile Ad hoc Networks are of following types:

- Passive attack
- Active attack
- Layer Based Attack
- Multi-Layer Attack

1. Passive attack

A passive attack does not cause disturbance in the working of communication network.
E.g. Snooping: Snooping is unlawful accessibility to other person's information.

2. Active attack

An active attack tries to change or terminate the data which is communicated.

3. Layer based attack

Network Layer Attack:
The various network layer attacks are as follows:

- Wormhole Attack: In wormhole attack, a harmful device, obtains packs at a site in the network and channels them to some other site in the network, where these packs are again send into the network. This channel amid two conspiring assaulters is called as wormhole.
- Black hole Attack: An attacker takes note of the appeals for the routers in a flooding based protocol after the assaulter collects a appeal for a path to the destination device, it makes a reply with a very small path and comes in the track to do anything with the packs in flowing-out flowing a midst them.
- Byzantine Attack: Here, a bargained middle device or a resource of conceded midway device interferes with other devices and makes assaults for example generating direction-finding loops, dispatching packs on un-optimized paths and deliberately selects some packs to abandon which causes lowering down of the direction-finding facilities.
- Resource Consumption Attack: Here an assaulter uses and rubbishes assets of the devices available in the network. The assets rubbished are:
  - Battery power
  - Band width
  - Computational power

Routing Attack: There are different assaults on the path finding protocols which disturb the normal functioning of the network. List of such assaults is following:

i. Routing Table Overflow: Here, the assaulter creates makes paths to non-existing devices, with the objective of making too many paths to stop making of new paths or to devastate the protocol.
ii. Packet replication: here, an assaulter duplicates decayed packs.
iii. Route Cache Poisoning: Here, the path cache is annihilated.
iv. Rushing Attack: On-Demand Protocols (like AODV or DSR) which try replica over powering in path finding phase are susceptible to the assault.

Transport Layer Attack:

- Session Hijacking: Initially, the assaulter receives the IP address of targeted device and finds the right order number. On doing this, he performs s DOS assault on the victim. Consequently, the target system is in accessible for some period. The assaulters carry on the session with the other device as a lawful device.

Application Layer Attack:

- Repudiation: Repudiation is the rejection or tried rejection by a device associated fully or partially in the sending/receiving of info over network.

4. Multi-Layer Attack

- Denial of service (DoS): Here, an assaulter seeks to stop lawful and sanctioned users from accessing the facilities of network.
- Jamming: Here, the assaulter first tracks the wireless medium to find threat of getting signals by destination device. After that it sends signals at that rate causing reception at receiver's end without any mistake to be stuck.
- SYN Flooding: Here, a harmful device transmits SYN packs in large number to the target node, tricking the coming back address of the SYN packs.
- Distributed DOS Attack: Distributed Denial of Services is worst variety of DoS.

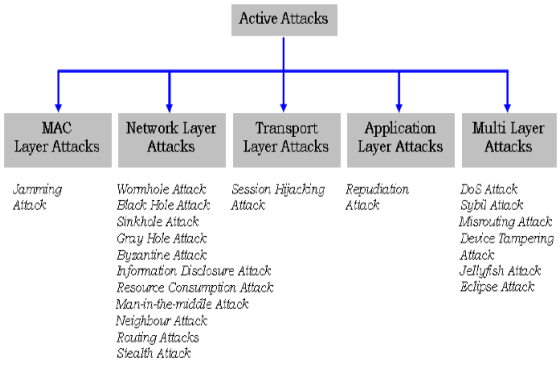

Fig-3: Classification of Security Attacks

IV. PROPOSED METHOD

The sub divisions list the various steps against the routing assaults and protected direction-finding conventions in Mobile Ad hoc Networks.

1. Intrusion Finding:

This methodology involves scattered and collaborative structure to notice the assault. All the devices in the MANETs are involved in this methodology. It finds the sign of invasion in the vicinity and self-sufficiently and also broadcasts this info to the other devices in the network.

2. Flooding Assault:

It is one of the easy methods to stop flooding assaults in AODV rules. Every device tracks its nearby devices RREQ. If the RREQ rate of a nearby device goes beyond the predefined boundary value, the device puts the identification key of that nearby device as blacklisted. Every upcoming RREQ from the blacklisted devices are abandoned. This method has drawbacks that a flooding boundary has to be predefined such that below that level assaults cannot be found out. Moreover, if a authentic devices identification is copied by a harmful device and a huge quantity of RREQs, are sent all over the network, other devices have the chances to make the identification of this authentic device as blacklisted.

Other adjective methodology is to lessen the consequence of flooding assaults in the AODV conventions. It uses a statistics to find RREQ floods and escape the progressing of those packs. This methodology is similar but dissimilar also in the sense that boundary value is found out based on statistical study of RREQ's and not maintain a predefined boundary value. The main benefit of this scheme is that it is able to lessen the negative outcome of changing flood frequencies.

A stream centred method is suggested for discovery of the flooding assaults in Mobile Ad hoc Networks involving the non-parameter procedure. In case of the assaults where the sender and receiver device addresses are created haphazardly for flooding (address spoofing), the writers have built a discovery piece as the fraction of new RREQ flows from the total RREQ flows, over a small time period. This fraction over time should keep on steady. For non-address spoofing attacks, in which case the flooding RREQ have matching sender and receiver device addresses, the discovery piece is built as the fraction of RREQ with a static group of sender and receiver node addresses to the total RREQ flows over a small span of time. This fraction over time should keep on steady. These fraction variables being haphazard, is used to find out boundary value for the case of assault.

A responsibility centred is deal Companionship has suggested to lessen the flooding and pack abandon assaults in Mobile Ad hoc Networks. They gave definitions of Rate Limitation, Enforcement and Restoration as the perfect parameters of Companionship. A faith or safety convention is to be implemented along with Companionship to increase the safety and efficiency in Mobile Ad hoc Networks.

3. Black-hole Attack:

The methodology have been suggested for appealing device with not directing the DATA packs to the response device immediately pauses for other responses with next jump particulars from the nearby devices. On receipt of the first appeal a clock is set in the Clock-Expired-Sheet, for getting more appeals from other devices. The 'order number', and the time at which the pack reaches is maintained in a 'Collect Route Reply Table' (CRRT). Now the 'timeout' value centred on incoming time of the first path appeal are obtained. Then CRRT is tested for any recurrent next jump device .If present, it is supposed the paths are right or the probability of harmful path is less. If there is no recurrence, any haphazard path from CRRT is carefully chosen.

Other methodology has been suggested- the path confirmation request (CREQ) and path confirmation reply (CREP) to evade the black-hole attack. The intermediary device apart from transmitting RREPs to the sender device, also directs CREQs to its next-jump device on the way to the receiving device. The next-jump device on receiving of a CREQ searches its cache for path to the receiving device. If it is present, it transmits the CREP to the sender. Then, the receiving device matches the path in RREP and the one in CREP. If the two are alike, the sender device announces the path to be right. It will not work for black-hole assaults, if 2 successive devices work in agreement, that is, when the next-jump device is a conspiring attacker.

Other methodology has been suggested- the sender devices to pause till the coming of a RREP pack from more than two devices. After receipt of many RREPs, the sender device tests about a shared jump. If at least one jump is collective, the sender node tells that path is secure. The limitation is the delay.

The black-hole attack and propounded that the receiver order number be satisfactorily grown by the assaulter device to assure the sender device that the path outputted is optimal. Based on differences between the destination sequence numbers of the received RREPs, the writers suggested a statistics centred abnormality discovery tactic to notice the black-hole assault. The tactic has a benefit that the assault is discovered at a minimal price and no extra direction-finding movement no change of current conventions, only the false positives are a disadvantage.

4. Worm Hole Attack:

To protect against this, it is suggested time-based chains and terrestrial chains. In case of time-based chains every device calculates the pack termination time centred on the speed of light c and is to involve it in the pack to going more than a particular distance, L. At the destination device, the pack is tested for pack termination by matching its current time and the termination time in the pack. The writers also suggested TIK, to validate the termination time that can be changed by harmful device. The restriction is that all devices have to be in tight clock synchronization. In case of the terrestrial chains, all devices must know its location and can be in loose timer synchronization. Here, a pack transmitter involves its current location and the transmitting time. So, a receiving

device tries to find the associations with nearby devices via calculation of distance between itself and the transmitting source. The benefit of terrestrial chains over time-based chains is the non-criticalness of time synchronization.

Other methodology suggested statistics related study of Multi route, to find the wormhole assault via multi path direction-finding. The assault is found out via computation of the comparative rate of every bond in every path found out in one path uncovering. The bond having the greatest comparative rate is treated as the wormhole bond.

Other methodology has proposed scheme centred on circulation quickness of appeals and statistical summarizing. For on call path finding system switch apply flooding, appeals should be communicated at a greater significance than all other packs. Thus the time to give-and-take info amid harmful devices grows. A scattered and adjusting statistic related summarizing method to sieve RREQs (all receiver devices sieves RREQs directed to it and have disproportionately great postponements) or RREPs (all sender device tracks the RREPs it accepts and sieves those having disproportionately great postponements) is recommended. Because diverse RREQs/RREPs have changing number of jumps, the upper boundary value on the jump time of RREQ/RREP packs is computed in such a way that most standard packs are taken and most untrue packs are sieved. There al benefits of this scheme are that globally network synchronized timers are not needed, there is no extra control pack overload and only easy calculations through the sender or receiver devices is needed.

Other methodology concentrates on the abnormality in the Mobile Ad hoc Network movement manners, especially the abnormality with manners in the conventions associated packs for finding worm holes. The HELLO note break was scheduled to 0.3 seconds, along a jitter function – haphazardly getting 0.03seconds of extra postponement. The movement is parsed, the HELLO communications incoming at a special devices are numbered, and the result of subtraction amid advent times of HELLO messages sent by its neighbours is calculated. The HELLO Message Timing Interval HMTI summary acquired is applied for finding assaulter devices, because the rate summary of HMTI is at a predefined rate, an abuse to OLSR conventions conditions. The break between the packs is frequently greater than it should be for an authentic device.

Layers	Assaults	Way out
Application Layer	Repudiation, data corruption	Finding and stopping virus, worms, harmful programs and application misuses by applying of Firewalls, IDS.
Transport Layer	Session takeover, SYN Flooding	Verification and validation, safeguarding end-to-end or point-to-point messaging use of public cryptography(SSL, TLS, PCT) etc.
Network Layer	Routing protocol attacks (e.g. DSR, AODV etc.),Wormhole, black-hole, Byzantine, flooding, resource consumption, location disclosure attacks	Shielding the ad hoc direction-finding and further in conventions
Data Link Layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness etc.	Defending the wireless MAC conventions and giving link layer safety maintenance.
Physical Layer	Eavesdropping, Jamming, interceptions	Stopping signal jamming denial-of-service assaults by using Spread Spectrum Mechanism.

Table-1: Security Solutions for MANET

V. RESULTS AND DISCUSSION

Mobile ad hoc Network have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. Due to ability and open media nature, the mobile ad hoc networks are much more prone to all kinds of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wires networks. This paper highlights the some typical vulnerability which are caused by characteristics of mobile ad hoc networks such as dynamic topology, limited resources (e.g. bandwidth, power), lack of central management's points. And finally it discusses the active and passive security attacks on each layer and their solutions. This paper discusses the attacks which may happen in MANETs. It also focuses on the proposed techniques to prevent the attacks on MANET. The proposed mechanism

can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of attacks.

REFERENCES

[1] Umesh Kumar Singh, Shivlal Mewada, Lokesh Laddhani and Kamal Bunkar, "An Overview & Study of Security Issues in Mobile Ado Networks", International Journal of Computer Science and Information Security (IJCSIS) USA, Vol-9, No.4, pp (106-111), April 2011

[2] Bo-Cang Peng and Chiu-Kuo Liang "Prevention techniques for flooding attack in Ad Hoc Networks", IEEE, 2006

[3] Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris, "A High-Throughput Path Metric for Multi-Hop Wireless routing", in ACM Mobicom, 2003.

[4] D.M. Shila, and T. Anjali, "Defending selective forwarding attacks in WMNs", IEEE International Conference on Electro/Information Technology, 2008, 96-101.

[5] X.P. Gao; and W. Chen, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks[C]", IFIP International Conference on Network and Parallel Computing Workshops, 2007, 209-214.

[6] Hongmei Deng, Wei Li, and Dharma P.Agrawal,"Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, vol. 40,Issue: 10, 2002

[7] Tamilselvan L, and Sankaranarayanan V, "Prevention of Black hole Attack in MANET", Paper presented at the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.

[8] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues (IJCSI), Vol. 2, Issue 3, pp.: 54-59,

[9] Nital Mistry, Devesh C Jinwala, Member, IAENG, and Mukesh Zaveri, "Improving AODV Protocol against Black hole Attacks", IMECS2010

[10] Hakem Beitollahi ⇑, Geert Deconinck (2012), Analysing well-known countermeasures against distributed denial of service attacks, Elsevier journal, vol 35, pages 1312-1332.

[11] Ningrinla Marchang a, Raja Datta (2008), Collaborative techniques for intrusion detection in Mobile ad-hoc networks, Elsevier journal, vol 6, pages 508-523.

[12] Sudip Misra, P. Venkata Krishna,_, Kiran Isaac Abraham, Navin Sasikumar, S. Fredun(2010), An adaptive learning routing protocol for the prevention of distributed denial of service attacks in wireless mesh networks, Elsevier journal,vol. 60,pages 294-306.

[13] Hung-Jen Liao, Chun-HungRichardLin, Ying-ChihLin, Kuang-YuanTung (2013), Intrusion detection system: A comprehensive review, Elsevier journal, vol.36, pages 16-24.

[14] Shelly Xiaonan Wu, Wolfgang Banzhaf (2010), the use of computational intelligence in intrusion detection systems: A review, Elsevier journal, vol.10, pages 1-35

[15] Adrian P. Lauf, Richard A. Peters, William H. Robinson(2010), A distributed intrusion detection system for resource-constrained devices in ad-hoc networks, Elsevier journal,vol.8,pages 253-266

Authors Profile

Mr.Omkar R Vaidya is student School of Computing Science and Engineering at V.I.T. University, Vellore, India. He received his BE (Information Technology) from Shivaji University and pursuing M.Tech. (Computer Science and Engineering) from Vellore Institute of Technology. He has participated in the National Programming Contest and National Level Debate held at Shivaji University. He won 2 prizes at National Level Programming Context. His area of interest is MANET and its issues, Programming.

Gautam Amiya completed B.E in Computer Science and Engineering from Sri Venkateshwara College of Engineering in Bangalore, Karnataka in the year 2013.Currently, he is pursuing M.Tech in Computer Science and Engineering from VIT,Vellore. His areas of interest are networks security, artificial intelligence and neural networks.

Dr.N.Jaisankar is Professor in the School of Computing Science and Engineering at V.I.T. University, Vellore, India. He received his BE (Computer Science and Engineering) from Bharathiar University in M.E. (Computer Science and Engineering) from M.K.University and Ph.D (Computer Science and Engineering) from VIT University. He has 18 years of experience in teaching and research. He was the Head of the department of Information Technology at KSRCT, Tiruchengodu, India. He is a Cisco Certified Network Associate Instructor and SUN certified JAVA instructor. He has reviewed many books titled Network Security, Data Mining, TCP/IP protocol suite and Programming in JAVA. He has participated as a coach in the International Programming Contest held at IIT, Kanpur, India. He has published many papers in International and national Journals and conferences on Network Security. Computer Networks and Data Mining. His research interest includes Computer Networks, Network Security, Network Protocols, Wireless Mobile Ad hoc Network and Data Mining. He has serverd in many international Journals as an editorial board member, Guest handling editor, advisory board member and reviewer etc. Also he has served in many international conferences as General chair, International advisory board member, technical program committee member, publication chair, organising committee member, reviewer etc. He is a life member of Indian Society for Technical Education, Computer Society of India , International Association of Computer Science and Information Technology, International Society for Research in Sciene and Technology and member of International Association of Engineers.