INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A STUDY ON SECURITY CHALLENGES IN MOBILE ADHOC NETWORKS

S.Banu Priya[1], C.Theebendra[2]

[1]M.Phil Research Scholar, annusavi72@gmail.com
[2] Assistant Professor, theebendra@gmail.com
Department of Computer Science, Vivekanandha College of arts and science for women (Autonomous), Namakkal (TN), India

Abstract: - MANET is a kind of AdHoc network with mobile, wireless nodes. Because of its special characteristics like dynamic topology, hop-by-hop communications and easy and quick setup, MANET faced lots of challenges allegorically routing, security and clustering. The security challenges arise due to MANET's self-configuration and self-maintenance capabilities. In this paper, we present an elaborate view of issues in MANET security. Based on MANET's special characteristics, we define three security parameters for MANET. In addition we divided MANET security into two different aspects and discussed each one in details. A comprehensive analysis in security aspects of MANET and defeating approaches is presented. In addition, defeating approaches against attacks have been evaluated in some important metrics. After analyses and evaluations, future scopes of work have been presented.

Keywords: Mobile AdHoc Network (MANET), Security, Attacks on MANET, Security services, Survey.

1. Introduction

In these years, progresses of wireless technology and increasing popularity of wireless devices, made wireless networks so popular. Mobile AdHoc Network (MANET) is an infrastructure - independent network with wireless mobile nodes. MANET is a kind of AdHoc networks with special characteristics like open network boundary, dynamic topology, distributed network, fast and quick implementation and hop-by-hop communications. These characteristics of MANET made it popular, especially in military and disaster management applications. Due to special features, wide-spread of MANET faced lots of challenges. Peer to peer applications [1], integration with internet [2], security [3], maintaining network topology [4] and energy [5,6] are some of the most important challenges in MANET. We presented an analysis and discussion in MANET challenges in our previous work [7].

In MANET all nodes are free to join and leave the network, also called open network boundary. All intermediate nodes between a source and destination take part in routing, also called hop-by-hop communications. As communication media is wireless, each node will receive packets in its wireless range, either it has been packets destination or not. Due to these characteristics, each node can easily gain access to other nodes packets or inject fault packets to the network. Therefore, securing MANET against malicious behaviors and nodes became one of the most important challenges in MANET [8].

2. Important Parameters in MANET Security

Because of MANET's special characteristics, there are some important metrics in MANET security that are important in all security approaches; we call them "Security Parameters". Being unaware of these parameters may cause a security approach useless in MANET. Figure1 shows the relation between security parameters and security challenges. Each security approach must be aware of security parameters as shown in Figure1. All mechanisms proposed for security aspects, must be aware of these parameters and don't disregard them, otherwise they may be useless in MANET. Security parameters in MANET are as follows

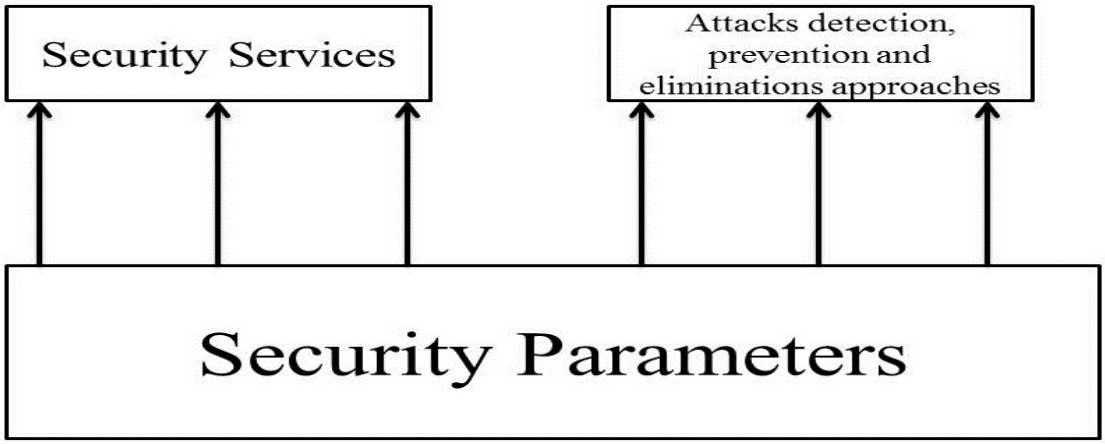

Figure1.Relation between Security Parameters and Security aspects

Network Over head: This parameter refers to number of control packets generated by security approaches. Due to shared wireless media, additional control packets may easily lead to congestion or collision in MANET. Packet lost is one the results of congestion and collision. Therefore, high packet overhead increases packet lost and the number of retransmitted packets. This will easily wastes nodes energy and networks resources.

Processing Time: Each security approach needs time to detect misbehaviors and eliminate malicious nodes. Due to MANET's dynamic topology it's strongly possible that routes between different nodes break because of mobility. Therefore, security approaches must have as low as possible processing time in order to increase MANET flexibility and avoid rerouting process.

Energy Consumption: In MANET nodes have limited energy supply. Therefore, optimizing energy consumption is highly challengeable in MANET. High energy consumption reduces nodes and network's lifetime.

Each security protocol must be aware of these three important parameters. Security protocols that disregard these parameters aren't efficient as they waste network resources.

3. MANET Security Challenges

One of the earliest researches in security in MANET was presented in 2002 [9]. Some security challenges in MANET were in herited from adhoc networks that were research interests since 1999[10, 11]. Generally there are two important aspects in security: Security services and Attacks. Services refer to some protecting policies in order to make a secure network, while attacks use network vulnerabilities to defeat a security service. In the next two parts, a brief discussion on these security aspects is presented.

3.1 Security Services

The aim of a security service is to secure network before any attack happened and made it harder for a malicious node to breaks the security of the network. Due to special features of MANET, providing these services faced lots of challenges. For securing MANET a trade-off between these services must be

provided, which means if one service guarantees without noticing other services, security system will fail. Providing a trade-off between these security services is depended on network application, but the problem is to provide services one by one in MANET and presenting away to guarantee each service. We discuss five important security services and their challenges as follows:

Availability: According to this service, each authorized node must have access to all data and services in the network. Availability challenge arises due to MANET's dynamic topology and open boundary. Accessing time, which is the time needed for a node to access the network services or data is important, because time is one of the security parameters. By using lots of security and authentication levels, this service is disregarded as passing security levels needs time.

Authentication: The goal of this service is to provide trustable communications between two different nodes. When an ode receives packets from a source, it must be sure about identity of the source node. One way to provide this service is using certifications, who ever in absence of central control unit, key distribution and key management are challengeable. In [13] the authors presented a new way based on trust model and clustering to public the certificate keys. In this case, the network is divided in to some clusters and in this clusters public key distribution will be safe by mechanisms provided in the paper. Their simulation results show that, the presented approach is better than PGP. But it has some limitations like clustering. MANET dynamic topology and unpredictable nodes position, made clustering challengeable.

Data confidentially: According to this service, each node or application must have access to specified services that it has the permission to access. Most of services that are provided by data confidentially use encryption methods but in MANET as there is no central management, key distribution faced lots of challenges and in some cases impossible.

Integrity: According to integrity security service, just authorized nodes can create, editor delete packets. As an example, Man – In – The – Middle attack is against this service. In this attack, the attacker captures all packets and then removes or modifies them.

Non-Repudiation: By using this service, neither source nor destination can repudiate their behavior or data. In other words, if a node receives a packet from node 2, and sends a reply, node 2 cannot repudiate the packet that it has been sent.

3.2 Attacks

Due to special features like hop-by-hop communications, wireless media, open border and easy to setup, MANET became popular for malicious nodes. Some of the most important attacks in MANET are as follows:

Black Hole Attack: In this attack, malicious node injects fault routing information to the network and leads packets toward it, then discards all of them [17-19]. In [20] we present a survey on black hole detection and elimination approaches. Also we presented a classification of defeating approach for this attack.

Worm Hole Attack: In worm hole attack, malicious node records packets at one location of the network and tunnels them to another location [22].Fault routing information could disrupt routes in network [23].

Byzantine attack: In this attack, malicious node injects fault routing information to the network, in order to locate packets in to a loop [25, 26]. One way to protect network against this attack is using authentication.

4. IN CORPORATING SECURITY AND OTHER CHALLENGES:

One way to provide security in MANET, besides decreasing network overhead, is to incorporate security approaches with other challenges. In this way, both challenges are solved by improving security parameters in total. We discuss these combinational approaches as follows:

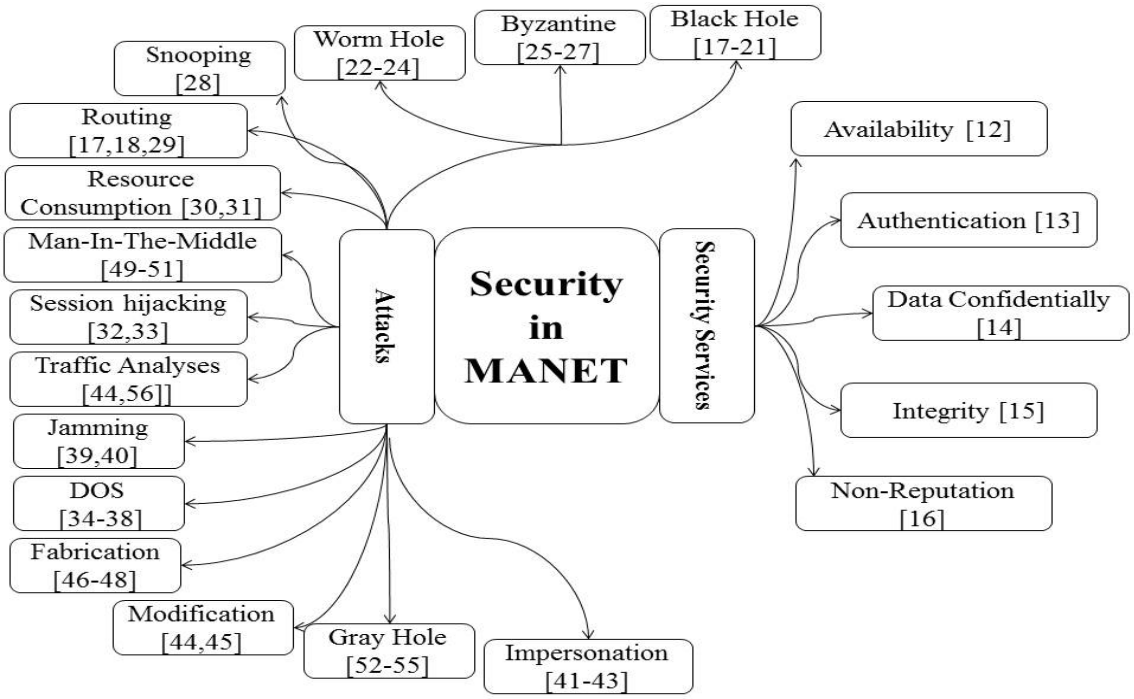

Figure2.SecurityAspectsinMANET

5. ANALYSES AND DISCUSSION :

Previous sections discussed in corporating security challenge with other challenges. This section presents an analytics and classification on previous issues. In order to analyses attacks and their behavior, an analyses in each attack is presented in Table1. For each attack five important parameters has been discussed. These parameters are as follows:

- Violated Service: Each attack breaks a security service. We presented the most important defeated service in this column.
- The Proposed Solutions: Some of the most effective approaches to detect and eliminate malicious nodes.
- MANET features which lead to this attack: Each malicious node uses a feature or features of MANET to break the security.
- Attack Type: Lots of researches classified attacks in two mainly class that are as follows: Active attack, Passive attack. In passive attacks, malicious node listens to transmissions without any active injection or effect on network [63]. While, in active attacks malicious node inject information.
- Attack Goal: The most important goal of each attack.

6. FUTUREDIRECTIONSOFRESEARCHES

Until now we briefly discussed the security challenges in MANET and present some analytics in them. In this section we present open research issues.

Routing information approaches are suitable in all types of MANET. In this approach, reducing packet over head and processing time, beside increasing accuracy is an important challenge. By increasing accuracy, it can detect cooperative malicious nodes. With decreasing processing time of this approach MANETs flexibility will increase.

7. CONCLUSION:

Mobile AdHoc Network (MANET) is a kind of AdHoc network with mobile, wireless nodes. Due to its special characteristics like open network boundary, dynamic topology and hop-by-hop communications MANET faced with a variety of challenges. Since all nodes participate in communications and nodes are free to join and leave the network, security became the most important challenge in MANET.

REFERENCES

[1] A.Gantes and j.stucky, "A platform on a Mobile Adhoc Network challenging collaborative gaming, "international symposiumon collaborative technologies and systems, 2008.

[2] K.U.R.Khan,R.U.Zaman, and A.V.G.Reddy, "Integrating Mobile AdHoc Networks and the Internet challenges and a review of strategies," presented at the 3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE, 2008.

[3] M.Suguna and P.Subathra," Establishment of stable certificate chains for authentication in mobile AdHoc networks," presented at the International Conference on Recent Trends in Information Technology (ICRTIT), 2011.

[4] H.Nishiyama,T.Ngo, N.Ansari, and N.Kato, "On Minimizing the Impact of Mobility on Topology Control in Mobile Ad Hoc Networks, " Wireless Communications, IEEE Transactions, 2012.

[5] F.D.RANGO, M.FOTINO ,ANDS .MARANO, "EE-OLSR: ENERGY EFFICIENT OLSR ROUTING PROTOCOL FOR MOBILE AD-HOC NETWORKS, "PRESENTED AT THE MILITARY COMMUNICATIONS CONFERENCE, MILCOM,2008.

[6] K.DuandY.Yang, "Policy-Based Time Slot Assignment algorithm in a MANET (PBTSA)," presented at the 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, ASID, 2009.

[7] M.Achankunju, R.Pushpalakshmi,and A.A.Kumar,"Particles warm optimization based secure QoS clustering for mobile adhoc network,"in Communications and Signal Processing(ICCSP),2013International Conference on, 2013,pp.315-320.

[8] R.Sheikh,M.S.Chande,andD.K.Mishra,"Security issues in MANET:Are view, "presented at the Seventh International Conference On Wireless And Optical Communications Networks (WOCN),2010.

[9] H.Deng,W.Li,andD.P.Agrawal,"Routing security in wireless AdHoc networks, ,"Communications Magazine,IEEE,2002.

[10] Y.Z.a and W.Lee, "Intrusion Detection in Wireless AdHoc, "presented at the 6th Int'l. Conf .Mobile Comp.Net. MobiCom,2000.

[11] F.S.a and R.Anderson, "The Resurrecting Ducking: Security Issues for Ad-Hoc Wireless Networks " 7th Int'l. Wksp on Security Protocols. Proc., LNC, 1999.

[12] X.Zhao,Z.You,Z.Zhao,D.Chen,andF.Peng,"AvailabilityBasedTrustModelofClustersforMANET,"presented atthe7thInternationalConferenceonServiceSystemsandServiceManagement(ICSSSM),2011.

[13] E.C.H.Ngai and L.M.R," Trust and clustering-based Authentication Services in Mobile AdHoc networks, "presented at the proceeding of the 24th international conference on Distributed Computing systems Workshops 2004.

[14] W.Lou,W.Liu ,and Y.Fang, "SPREAD: enhancing data confidentiality in mobile adhoc networks, "presented at the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies ,2004.

[15] S.RanaandA.Kapil,"Security-Aware Efficient Route Discovery for DSR in MANET , "Information and Communication Technologies, Communications in Computer and Information Science,vol.101,pp.186-194,2010.

[16] X.Lv and H.Li,"Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks," Information Security, IET, vol.7, 2013.

[17] S.a.A.k.G,H.o.d.R.m, and S.Sharma, "A Comprehensive Review of Security Issues in Manets "International Journal of Computer Applications vol. 692013.

[18] V.P.andR.P.Goyal,"MANET:Vulnerabilities, Challenges, Attacks, Application, "IJCEM International journal of Computational Engineering & management, vol. 11,2011.

[19] A. MISHRA, R. Jaiswal, and S.Sharma, "A novel approach for detecting and eliminating cooperative blackhole attack using advanced DR I table in AdHoc Network,"presentedatthe3rdInternationalConferenceonAdvanceComputingConference(IACC),2013

[20] "Presented at the first regional conference on optimizing and oft computing n electronic and computer engineering, 2014.

[21] N.-W.Lo and F.-Protocol to Prevent Cooperative BlackHole Attack in MANET, "in Intelligent Technologies and Engineering Systems. vol. 234, J. JuangandY.-C.Huang, Eds. ,ed: Springer New York, 2013,pp.59-65.

[22] M.A.Gorlatova,P.C.Mason,M.Wang,and L.Lamont, "Detecting Wormhole Attacks in Mobile AdHoc Networks through Protocol Breaking and Packet Timing Analysis, "Military Communications Conference, IEEE, MILCOM,2006.

[23] S.Keer and A.Suryavanshi,"To prevent wormhole attacks using wireless protocol in MANET, "presented at the international Conference on Computer and Communication Technology (ICCCT), 2010.

[24] Z.A.Khan and M.H.Islam, "Wormhole attack: A new detection technique ,"presented at the international conference on Emerging Technologies(ICET),2012.
[25] M.Yu,M.C.Zhou,and W.Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments, "IEEE TransactionsonVehicularTechnology,vol.58
[26] G.Singla,M.S.Sathisha,A.Ranjan,S.D.,and P.Kumara, "Implementation of protected outing to defend by zantine attacks for MANET's, "International Journal of Advanced Research in Computer Science, vol.3,p.109,2012.
[27] G.Singla and P.Kaliyar,"A Secure Routing Protocol for MANETs against Byzantine Attacks, "Computer Networks & Communications (NetCom), Lecture Notes in Electrical Engineering, vol.131, pp.571-578, 2013.
[28] S.Shaw,K.Orea,P.Venkateswaran, and R.Nandi, "Simulation and Performance Analysis of OLSR under Identity Spoofing Attack for Mobile AdHoc Networks, "Computer Networks and Information Technologies Communications in Computer and Information Science, vol. 142, pp. 308-310,2011.
[29] B.Kannhavong,H.Nakayama,Y.Nemoto,andN.Kato,"Asurveyofroutingattacksinmobileadhocnetworks," WirelessCommunications,IEEETransactions, vol.14
[30] M.Abdelhaq, R.Hassan, and R.Alsaqour ,"Using Dendritic Cell Algorithm to Detect the Resource Consumption Attack over MANET, "Software Engineering and Computer Systems Communications in Computer and Information Science vol.181,pp.429-442,2011.
[31] L.Rajeswari,A.Prema,R.A.Xavier,and A.Kannan, "Enhanced intrusion detection techniques for mobile adhoc networks, "presented a the International Conference on Information and Communication Technology in electrical Sciences(ICTES),2007.
[32] A.K.Rai,R.R.Tewari, and S.K.Upadhyay, "different type of attacks on integrated MANET telnet communication, "international journal of computer science and security(IJCSS),vol.4.
[33] J.Y.Kim,H.K.Choi, and S.Song, "A secure and light weight approach for routing optimization in mobile IPv6, "EURASIP Journal on Wireless Communications and Networking-Special issue on wireless network security,vol.7,2009.
[34] Supriyaand M.Khari, "Mobile AdHoc Networks Security Attacks and Secured Routing Protocols: A Survey "Advances in Computer Science and Information technology .Networks and Communications Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 84,pp.119-124,2012.
[35] J.SoryalandT.Saadawi,"IEEE802.11Denial of Service attack detection in MANET, "Wireless Telecommunications Symposium (WTS), 2012.
[36] R.H.Jhaveri, S.J.Patel,and D.C.Jinwala, "DoS Attacks in Mobile AdHoc Networks: A Survey "presented at the Second International Conference on Advanced Computing & Communication Technologies (ACCT), 2012
[37] A.MichaelandNadeem,"Adaptiveintrusiondetection&preventionofdenialofserviceattacksinMANETs,"presentedattheIWCMC'09ProceedingsoftheInternationalConferenceonWirelessCommunicationsandMobileComputing,ConnectingtheWorldWirelessly,2009.
[38] J.SuandH.Liu,"Protecting Flow Design for DoS Attack and Defence at the MAC Layer in Mobile AdHoc Network, "Applied Informatics and Communication Communications in Computer and Information Science ,vol. 224,pp.233-240,2011.
[39] A.HamiehandJ.Ben- Othman ,"Detection of Jamming Attack sin Wireless AdHoc Networks Using Error Distribution, "presented at the International Conference on Communications, ICC'09.IEEE,2009.
[40] J.Benothman and A.Hamieh, "Defending method against jamming attack in wireless adhoc networks, "presented at the 34th Conference on Local Computer Networks, LCN,IEEE,2009.
[41] D.Glynos, P.Kotzanikolaou, and C.Douligeris,"Preventing impersonation attack sin MANET withmulti-factor authentication, "hird International Symposium on Modelling and Optimization in Mobile, AdHoc, and Wireless Networks, WIOPT,2005.
[42] C.Douligeris,P.Kotzanikolaou, and D.Glynos, "Preventing Impersonation Attacks in MANET with MultiFactor Authentication, "WIOPT'05 Proceedings of the Third International Symposium on Modelling and Optimization in Mobile, AdHoc ,and Wireless Networks, 2005.
[43] M.Barbeau,J.Hall, and E.Kranakis, "Detecting Impersonation Attacks in Future Wireless and Mobile Networks, "Secure Mobile Ad-hoc Networks and Sensors Lecture Notes in Computer Science, vol.4074, pp.80-95,2006.
[44] N.Dixit, S.Agrawal, and V.K.Singh, "A Proposed Solution for security Issues In MANETs, "International Journal of Engineering Research &Technology(IJERT),vol. 2,2013.
[45] Vaithiyanathan, S.R.Gracelin, E.N.Edna, and S.Radha, "A Novel Method for Detection and Elimination of Modification Attack and TTL Attack in NTP Based Routing Algorithm, "presented at the International Conference on Recent Trends in Information, Telecommunication and Computing (ITC), 2010

[46] P.Yi,X.Jiang ,and Y.Wu, "Distributed intrusion detection for mobile AdHoc networks, "Journal on Systems Engineering and Electronics, IEEE,vol.19, 2008.
[47] S.R.Afzal, S.Biswas, J.B.Koh, T.Raza, and m. authors, "RSRP: A Robust Secure Routing Protocol for Mobile AdHoc Networks, "presented at the Wireless Communications and Networking Conference, WCNC, IEEE, 2008.
[48] P.T.Tharani, K.Muthupriya ,and C.Timotta,"Secured consistent network for coping up with fabrication attack in MANET, "international journal of Emerging Technology and Advanced Engineering, vol.3, 2013.
[49] D.Sharma, P.G.Shah, and X.Huang, "Protecting from Attacking the Man-in-Middle in Wireless Sensor Networks with Elliptic Curve Cryptography Key Exchange, "presented at the NSS'10 Proceedings of the Fourth International Conference on Network and System Security, 2010.
[50] K.Vishnu,"A new kind of transport layer attack in wireless AdHoc Networks, "presented at the International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010
[51] X.Zou,A.Thukral, and B.Ramamurthy,"An Authenticated Key Agreement Protocol for Mobile AdHoc Networks, "Mobile Ad-hoc and Sensor Networks Lecture Notes in ComputerScience,vol.4325,pp.509-520,2006.
[52] J.Liu,F.Fu,J.Xiao,andY.Lu,"SecureRoutingforMobileAdHocNetworks,"presentedattheEighthACISInternationalConferenceonSoftwareEngineering,ArtificialIntelligence,Networking,andParallel/DistributedComputing,SNPD,2007.
[53] J.Sen,B.Tata,M.Chandra,S.Harihara,and H.Reddy, "A mechanism for detection of grayhole attack in mobile AdHoc networks, "presented at the 6th International Conference on Information, Communications & Signal Processing, 2007
[54] G.Usha and S.Bose, "Impact of Grayhole attack on adhoc networks, "presented at the International Conference on Information Communication and Embedded Systems (ICICES), 2013
[55] G.Xiaopeng and C.Wei, "A Novel GrayHole Attack Detection Scheme for Mobile Ad-Hoc Networks, "presented at the IFIP International Conference on Network and Parallel Computing Workshops, NPC Workshops, 2007.
[56] C.Gray,J.Byrnes,and S.Nelakuditi, "Pairwise Resistence to traffic Analysis in MANETs, "ACMSIGMOBILE Mobile Computing and Communications Review, 2008.
[57] E.A.Panaousis, T.A.Ramrekha,and C.Politis, "Secure routing for supporting AdHoc extreme emergency infra structures, "Future Network and Mobile Summit, 2010.
[58] M.Salmanian and M.Li, "Enabling secure and reliable policy based routing in MANETs, "presented at the military communications conference, MILCOM, 2012.
[59] F.R.Yu, H.Tang,S.Bu,and D.Zheng, "Security and quality of service (QoS) co design in cooperative mobile adhoc networks,"EURASIP Journal on Wireless Communications and Networking-Special issue on wireless network security, 2013.
[60] R.Gujral, A.Kapil, and, Volume, ,pp "Secure QoS Enabled On Demand Link State Multipath Routing in MANETs, "Information Processing and Management Communications in Computer and Information Science, vol. 70,pp.250-257,2010.
[61] A.ElSayed,"Clustering Based Group Key Management for MANET, "Advances in Security of Information and Communication, Networks Communications in Computer and Information Science, vol.381, pp.11-26,2013.
[62] M.S.Zefreh, A.Fanian, S.M.Sajadieh, P.Khadivi ,and M.Berenjkoub, "A Cluster-Based Key Establishment Protocol for Wireless Mobile AdHoc Networks, "Advances in Computer Science and Engineering Communications in Computer and Information Science, vol.6, pp. 585-592,2009.
[63] L.Yingbin,H.V.Poor ,and Y.Lei, "Secrecy Throughput of MANETs Under Passive and Active Attacks, "Information Theory,IEEE Transactions on,vol.57,pp.6692-6702,2011.
[64] K.Gomathi and B.Parvathavarthini, "An efficient cluster based key management scheme for MANET with authentication,"inTrendz in Information Sciences & Computing (TISC), 2010, 2010, pp.202-205.
[65] A.ElSayed,"Clustering Based Group Key Management for MANET, "in Advances in Security of Information and Communication Networks. vol.381, A.Awad, A.Hassanien, and K.Baba, Eds.,ed:Springer Berlin Heidelberg, 2013,pp. 11-26.
[66] W.El-Hajj,D.Kountanis,A.Al-Fuqaha,andM.Guizani,"AFuzzy-Based Hierarchical Energy Efficient Routing Protocol for Large Scale Mobile AdHoc Networks (FEER), "in Communications, 2006. ICC'06. IEEE International Conference on, 2006, pp.3585-3590.