American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-3, Issue-10, pp-41-47
www.ajer.org

Research Paper Open Access

Black Hole and Greyhole Attack in Wireless Mesh Network

[1]Rupinder Kaur, [2]Parminder Singh
Student, IT Deptt.CEC, Landran, Mohali,
Assit.Professor,IT Deptt, CEC, Landran, Mohali,

Abstract: *Security is an important need in wireless mesh networks to give safe and shared information between wireless non-static nodes. In wireless network nodes has ability to act correctly and route the packets. Wireless mesh networks unusual method of producing,keeping and sharing information ability of mobile objects to show spontaneous and cheap adjusting arrangement itself.There are different types of communication devices in technology by which performance is measured.There is a major issue which take part in network and provide security from various kinds of malicious attacks.There are various attacks such as black hole attack,wormhole attack,Greyhole attack, and evesdropping attack.Black hole and Greyhole attacks are network layer attacks that spoils the performance by falling the packets.The black hole and Grey hole are the problem of security that consider in wireless networks.Black hole and Greyhole attack is one type of way of interrupting attack and can cause large amount of damage to network.Black hole attack is act like ad-hoc network; which create network and attack on packets.In black hole attack where a false node not make correct paths in public to receiver node during the direction finding process. Theattacker achieves this attack when all the similar kinds of nodes communicate and make network to each other. It is very important to protectthe network layer from these attack which is also a great issues in wireless mesh network.*

Greyhole attack is very difficult to detect in wireless mesh network.In this paper,its an overview about black hole attack and grey hole in wireless mesh network and define problem statement about them. Secondly, its take study about related work in which many authors perform on these attacks and then its discuss about proposed method.Thirdly,the results are simulated carried out in OPNET simulator where black hole attack and grey hole attack shows the performance and Its analysis the throughput in network.

Keywords---Black hole attack, Grey hole attack,MRP, OLSR, RREQ, RREP,RERR,OPNET.

I. INTRODUCTION

Wireless mesh network is combination of independent nodes that shared information with each other by making a multi-hop radio network and keeping joined in a non-static manner.Network changes its topology suddenly and without reason.There is lack of system support where each node play role like router and different node connect anywhere and go away from the network at any time.Wireless mesh network is type of dynamic network structures.In different form,an object in classical wireless LAN,all nodes are dynamic and changes in topology is done suddenly in wireless mesh network,which cause difficult job to the security of wireless network.As a result,attacker joins the network and grabbed packets and leaves the network. Black hole and Greyhole attacks are the two traditional attack under wireless mesh network,which spoil the network topology and degrade the network performance. In this paper,Its analysis the behaviour of wireless network and IEEE 802.11b protocol and then Its focus on black hole attack and Grey hole attack which coming in network and then apply OLSR proactive routing protocol and analysis the effect of these attacks on network. To build the awareness of this paper which is not forgotten is well managed as follows:Part II,provide the study about related research work,which contain existing methods to solve the same problem or related problem.In Part III Its discuss about our proposed work and its advantages of OLSR protocol. In Part IV Its analysis and describe the environment which help to show our results. Alsoits discuss about the simulation parameters. A number of simulation results are provided to notice the performance of our proposed method. Lastly,Its make conclusion and future scope.

1.1 .BLACK AND GREY HOLE ATTACK

Black hole means incoming and outgoing of information is dropped ,without telling the source node that the information did not communicate with planned receiver node. Black hole attack as its name specifies that, the attacker attacks and discards the whole packets from receiver node. A black hole node done its job in the following strategies: one time RREQ(route request) and RREP(route reply) message is received by source node ,then attacker send RREP message directly and shows that it is real receiver node. The sender node having fake RREP from attacker, after that real RREP message is discarded. Under these condition, the sender node post packets to black hole in the place of receiver node. When the sender node transfers the packets through black hole, then attacker dropped them without replies as RERR (route error) message. The Grey hole present the same attitude and behaviour like black hole. The difference is that the Grey hole does not drop whole packets, it dropped some part of packets. The packets are dropped by false node which is known as attacker node. The black hole and Grey hole attack will carry a large amount of effect to the performance of wireless mesh network. In previous study, the authors bring out experiments on black hole and Grey hole by measuring its Grey magnitude. Grey magnitude means if It's have value of seed is 50 then its probability of dropping the packets is 50%.In part IV of this paper ,Its analyse the different behaviour of nodes.

II. RELATED WORK

JiItsn et al[13] presented the adaptive approach to detect black hole and grey hole attack in ad-hoc networks.They generated a Path based detection algorithm where each node not necessary watch all nodes,but it only observe the next node in current path.In this ,they analysis the false positive probability taking constant threshold and dynamic threshold.Also ,they analysis the great impact of performance under different grey magnitude values. Patcha et al[1] proposed a proper way of prevention of black hole attack.To handle collision among nodes they introduced the watchdog method.In this algorithm,nodes are divided into three parts in network i.e.trusted,watchdog and ordinary nodes.Every watchdog node that is chosen should watch carefully its normal node neighbours and notice whether they can be behaved as trusted or malicious node. Deng et al[11] have proposed a technique for detecting a malicious nodes which is present as a chain in ad-hoc network,that malicious node is known as black hole and Grey hole node.In this,total load traffic is categorised into small set of blocks and at initial step make a backbone of strong nodes on ad-hoc network.Strong nodes mean nodes having well in terms of radio range and power computing.Remaining nodes which are not considered as strong nodes is aregular node.The disadvantage of this technique is that the strong node consider as trusted node ,and if attacker attack on that nodes;then algorithm is failed and black hole and Grey hole is generated. Geo et al[22] presented aggregate signature algorithm to trace packet dropping nodes. Theybind up into three algorithms.(1) creating proof algorithm.(2) The checkup algorithm.(3)The diagnosis algorithm. The advantage of this presented work are(1)The bandwidth overhead is low.(2) Thesecurity issues are fulfilled.(3) No need of bidirectional communication link.(4)There is broad scope for applications.

III. PROPOSED WORK

Black hole and Greyhole attack is a major problem in wireless mesh network.Our proposal is based on the analysing these attacks in 802.11b network environment and calculate is through put in both attack,that how black hole and Grey hole node effect the throughput.Its implement it by taking nodes as vector; i.e. one node is link with two nodes in x-axis and y-axis, and further make links as vector quantity. In this each node is connected to next nodes and packets broadcast it.Thereis all mobile nodes,which is not fixed in position and all nodes are connected with one IP called backbone.Firstly, it's make scenario of wireless nodes and deploys random way point on each node and then change wireless LAN parameters. It's give each node as unique basic service station number and also set channel for these service station and then transfer the packets and generate graph of network without attacks. Secondly,after that Its change one node as false node and generate black hole then transfer the packets and generate graph.by this false node our packets shows source value but receiver node value is zero,that means whole packets are dropped and at receiver node information is not retrived.Ater this, Its make that false node as Grey hole node,configure it by taking variable seeds and generate graph of that scenario.Finally Its configure this scenario by taking OLSR(optimized link state routing protocol) protocol in each statics then compare the performance.OLSR is also stored all the information in tables.It updates the topology of network which is changed in wireless mesh network.In network layer OLSR protocol accumulated throughput is calculated.

These all works has some advantages which are as follows:

1. In this, each node is connected to two nodes and all the information is stored in tables.
2. Its require no encryption on topology control, so information sharing is easy.
3. There is not necessary to watch all nodes, one node record link of just two nodes by which it link.

IV. SIMULATION ENVIRONMENT

The prevention is implementing in OPNET simulator and performance is analyzed in term of network throughput and load. Simulation of black hole and Greyhole attack on the OPNET is achieved by having a false node. This node is detected through secure path scheme having OLSR protocol in order to stop the behavior of false node. In following scenario which is set of 30 mobile nodes. These mobile nodes are moving with constant speed of 10 m/s and simulation time taken as 1000 seconds. Area of simulation is taken as 1500*1500 metersand mobility model is random way point with speed 10 m/s and transmitting power is by default 0.005 watts. The random environment is chosen in wireless mesh network and other specification of simulation isas follows:

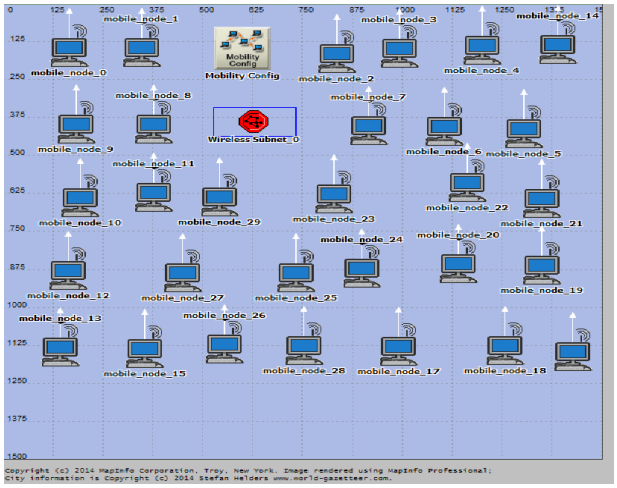

Fig 1. Scenario of 30 nodes

Fig 1, shows the scenario in which wireless subnet having address 255.255.192.2 by which 30 nodes are connected and communicate.The host address of node is starting from 192.168.5.0/26,192.168.5.130,192.168.5.64 and end at 192.168.5.65 .These nodes communicate with the help of broadcast ip address ,i.e192.168.5.63 .Our main goal is to check which attack is more dangerous effect on network performance .The last but not least stage and very vital of the time is given to this stage.

V. SIMULATION RESULTS

In random simulation environment, the first step is to determine the throughput and network load on network performance.Results are analysed carefully by obtaining from OPNET simulation.Its simulate anetwork of 30 mobile nodes.In OPNET there is set of two types of statics i.e. global and node.Initial take a uniform scenario with no black hole and grey hole attacks. There is no prevention is applied, then attacks will occurs. The false node is choose randomly in simulation test, and decreases the throughput and increases the network load on network. The simulation results are presented in fig 2. And fig 3; which shows the network performance without attacks and with both attacks,i.e. black hole and Grey hole attack as follows:

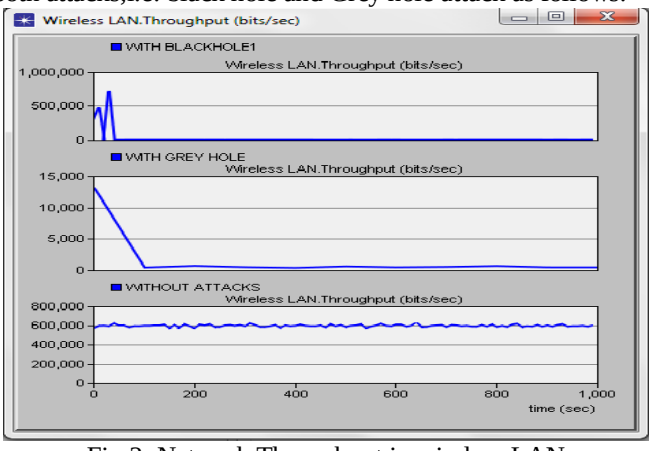

Fig 2: Network Throughput in wireless LAN

Firstly, in without attack graph itstransmits the packets in the form of bits from source to receiver node. After this Its generated one false node in network ,that false node is black hole or Grey hole node then performance of network is vary which shows as follows:

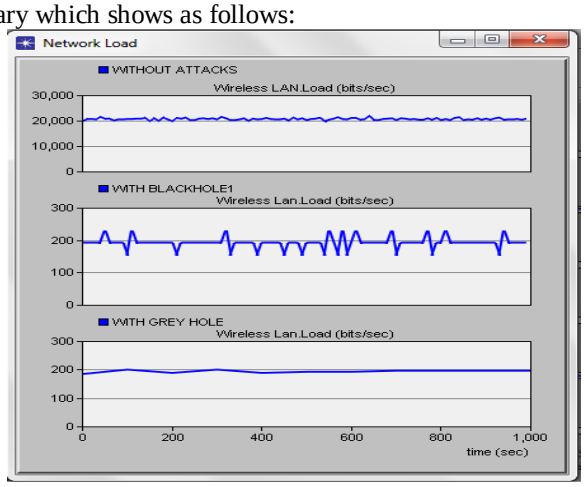

Fig 3: Network Load in wireless LAN

Based on these above results, Secure path prevention technique is generated and analysis the network performance.After implementingthe secure path scheme and prevent the network from attack and shows the drastic changes in the performance of throughput and network load. First its detect the node from route table that stored inOLSR table as shortest path. Its take that value from the table which does not show the route between source to receiver node which means attack will occur. Ifit'sfinding that kind of value, thenits drop that route and prevent network from attacks. The effect on throughput with attacks and after prevention is calculated as follows:

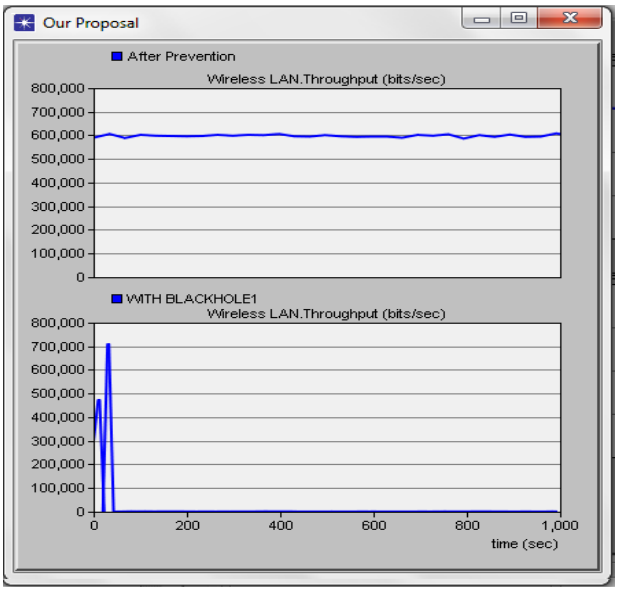

Fig 4: Network Throughput in black hole attack

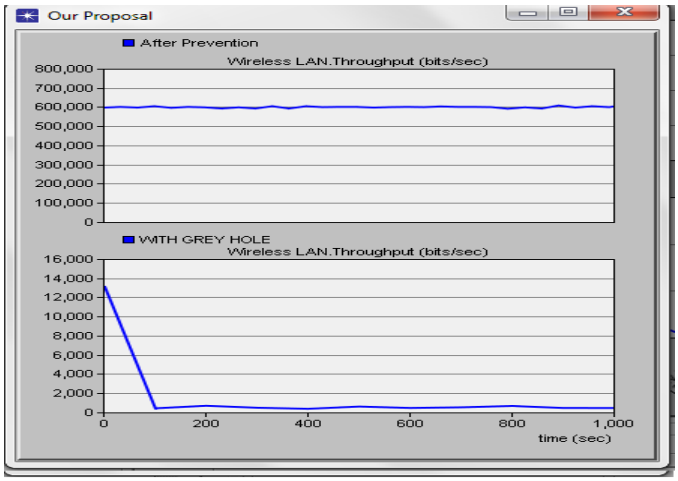

Fig 5: Network Throughput inGreyhole attack

This technique is provides good performance for detecting attacks and work without any modification of protocol and without special environment assumptions. When the nodes found no route to receiver node in table, that means attacks occurs and with the help of prevention technique it drop that route and improves the network performance. Black hole and grey hole attack is a routing layer attacks in which data is revolves from other node. The transmission of packets on multiple nodes and dropping of packets is mostly occurring on routing layer. Routing protocol is targeted by the attack. Greyhole attack having great influencing attack on Wireless mesh network.By this it also find variation in network load which show as following graphs.

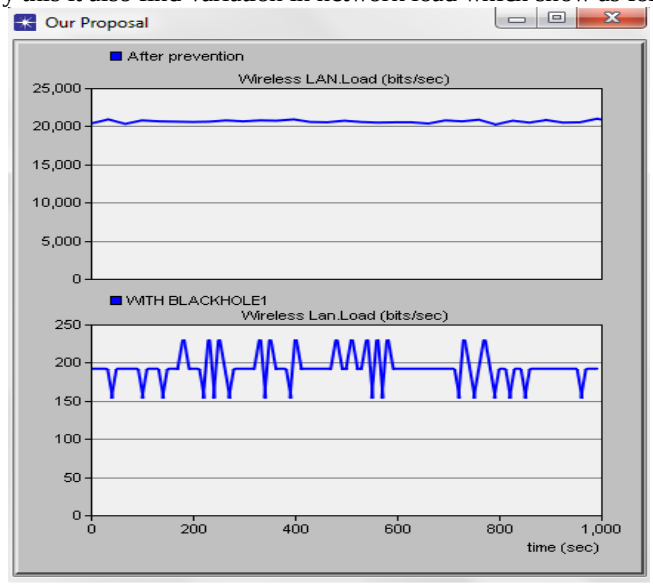

Fig 6:Network Load in black hole attack

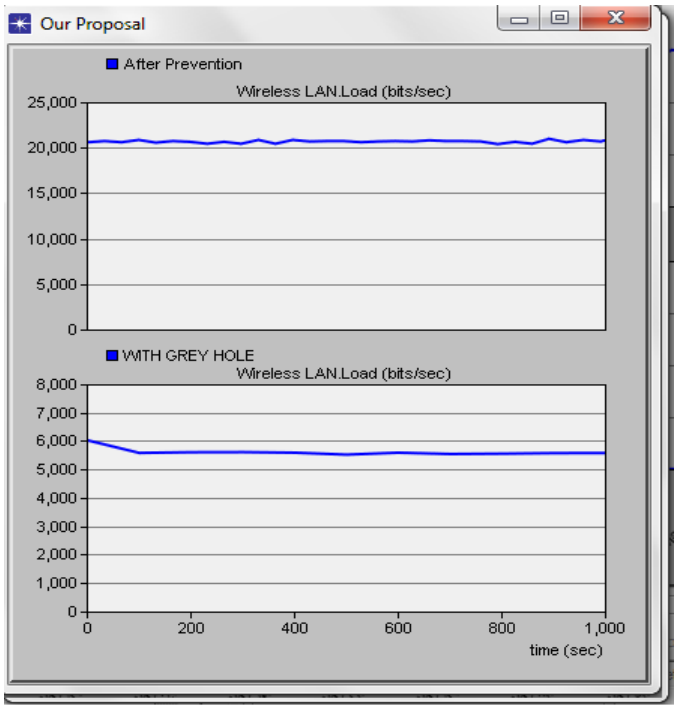

Fig 7: Network Load inGreyhole attack

VI. CONCLUSION

Security is the important feature in wireless mesh network.In this paper,the black hole and grey hole attack is come on network layer.due to movable nature,wireless mesh network have many Itsakness.Our aim is to prevent the network layer from these attack in which false node act as regular node.That node is difficult to detect, because the nodes here in this type of attack are very much unpredictable and volatile as they varies from normal to adversary and adversary to normal nodes.In this paper,Its apply OLSR protocol and find out that it stops some effect of these attacks,but Its cannot safe network from these attacks purely.Its also find that black hole attack is easy to detect than Grey hole attack.At performance level,there is not much difference in both attacks.

VII. FUTURE SCOPE

Network layer is full of attacks.If secure network layer then its safe many information from attackers.To study the related researches,its find how attack occur in network layer.Our main goal is to detect and present black hole attack and Greyhole attack and cause security better so that performance of network is not degrade.

REFERENCES

[1] A.Patcha, A.Mishra, "Collaborative Security architecture of black hole attack prevention in mobile ad hoc networks[C]",Radio and Wireless Conference,2003,pp.75-78

[2] B. Sun, Y. Guan, ,J. Chen ,U.W Pooch, "Detecting Black hole attack In Mobile Ad-hoc Netwoks[C]".5thEuropeenPersonel Mobile Communications Conference,2003,pp. 490-495.

[3] C. Karlof, D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures, Special Issue on Sensor Network Applications and Protocols", vol 1 (2-3), 2003,pp.1293 –1303

[4] Dr. A. A. Gurjar, Professor, Department Of Electronics & Telecommunication, Sipna's C.O.E.T, Amravat and A. A. Dande, Second Year (M.E.), Computer Engineering, Sipna's C.O.E.T, Amravat " Black Hole Attack in Manet's: A Review Study" International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 2, No. 3, March 2013,pp. 12-14.

[5] D.Djen, L. Khelladi, and A.N. Badache, "A survey of of Security issues in Mobile Ad Hoc Network," Communication Surveys & Tutorials , IEEE,vol. 7 no. 4, ,pp. 2-28,2005.

[6] D.Boneh,C.Gentry,B.Lynn,H.Shachem,"Aggregate and Verifiably Encrypted Signature from Bilineer Maps ",Advances in Cryptology-EUROCRYPT'03,LNCS 2656,Berlin,Spinger-Veralg,2003,pp.416-432.

[7] Elizabeth M. Royer, and Chai-KeongToh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, April 1999, pp. 46-55.

[8] F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, Apr, 2002, pp. 22-26.

[9] HesiriItserasinghe and HuirongFu,"Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks", International Journal of Software Engineering and Its Applications,Vol. 2, No. 3, July, 2008,pp.39-54.

[10] H. Deng, W. Li, and D. P. Agrawal."Routing Security in Adhoc Networks." In: *IEEE* Communications Magazine, Vol. 40, No. 10, Oct. 2002,pp. 70-75.

[11] Hongmei Deng, Itsi Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October 2002,pp70-75.

[12] J. Cai, P. Yi, J. Chen, Z. Wang, N. Liu, An adaptive approach to detecting black and Grey hole attacks in ad hoc network, in: 4th IEEE International Conference on Advanced Information networking and Applications, IEEE Computer Society, 2010, pp.775–780.

[13] JiItsn CAI,Ping YI,JialinCHEN,Zhiyang WANG,Ning LIU,"An adaptive approach to detecting black and Grey hole attacks in Adhoc networks",24th IEEE International Conference on Advanced Information networking and application,2010,pp.775-891.

[14] LathaTamilselvan,VSankaranarayanan,"Prevention Of Blackhole Attack in MANET",In proceeding of 3nd International Conference on Wireless Broadband and Ultra Wideband Communication, Aug 2007,pp.21-21

[15] 15] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attackin wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), Apr. 2004, pp. 96-97.

[16] N. H. Mistry, D. C. Jinwala and M. A. Zaveri,"MOSAODV: Solution to Secure AODV against Black hole Attack", (IJCNS) International Journal of Computer and Network Security, Vol. 1, No. 3, December 2009.pp.42-45.

[17] O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks", In Proceedings of the 36th Hawaii International Conference on System Sciences,2003, pp. 57-61.

[18] R.Agrawal, R. Tripathi, S. Tiwari, "Performance evaluation and comparison of aodv and dsr under adversarial environment", International Conference on Computational Intelligence and Communication Networks, IEEE Computer Society, 2011, pp.596–600.

[19] R.H.Jhaveri, S.J.Patel, D. Jinwala, "A novel approach for Greyhole and blackhole attacks in mobile ad hoc networks", Second International Conference on Advanced Computing and Communication Technologies, IEEE Computer Society, 2012, pp. 556–560.

[20] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. "Detecting Blackhole Attack on AODV based Mobile Ad hoc networks by Dynamic Learning Method". International Journal of Network Security, Vol.5, No.3,Nov 2007, pp.338–346.

[21] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy efficient communication protocol for wireless microsensornetworks",IEEE Transactions on Wireless Communications ,vol 1 (4) ,2002,pp. 660–670.

[22] X.P.Geo,W.Chen,"A Novel Grey hole Attack Detection Scheme for Mobile Adhoc Networks[C]",IFIP International Conference On Network and Parallel Computin Workshop,2007,pp. 209-214.

[23] Xiaoyan Hong, KaixinXu, and Mario Gerla, "Scalable Routing Protocols for Mobile Ad hoc Networks," IEEE Network,Vol.16(4),July/August2002,pp.11-21.

[24] Y. A. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French Riviera, Sept. 2004.

[25] Y. Zou, K. Chakrabarty, "Sensor deployment and target localization based on virtual forces", TItsnty- Second Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 2, IEEE Computer Society, 2003, pp. 1293–1303.

[26] Y. Law, P. J. Havinga, "how to secure sensor network", International Conference on Sensor Networks and Information Processing, IEEE Computer Society, 2010, pp. 89–95.

[27] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Adhoc Networks," Proc.4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June 2002, pp. 3-13.