ISSN: 2277 – 9043
International Journal of Advanced Research in Computer Science and Electronics Engineering
Volume 1, Issue 4, June 2012

A survey on Selfishness and Countermeasure in MANET

Purushottam Patel
Computer Science & Engineering
Thakral College of Technology
Bhopal, India
puru_patel123@rediffmail.com

Rupali Soni
Deptt. of Computer Science & Engineering
Thakral College of Technology
Bhopal, India
roopalisoni@oriental.ac.in

***Abstract*— Routing is a easiest way to launch a attack in MANET due to highly dynamic topology which makes routing procedure more complicated and insecure and therefore nodes are more susceptible to compromise and are particularly vulnerable to denial of service attack (DoS) attacks launched by malicious nodes or intruders .Another challenging issue is selfishness of a node which dramatically decreases the performance. On demand routing such as AODV is more popular then proactive routing use flooding to discover route. Attackers used this concept to launch DoS attack like flooding; black hole and gray hole are the known attack in MANET. In this article we have presented a descriptive surveyed on the MANET attacks specially attacks blows on route discovery phase. Finally this paper presents a proposed methodology to detect and restrict the selfishness using the support vector machine with threshold mechanism. The behavior is the key point to classify the characteristics of a node. Our proposed scheme will be implemented on NS-3 test bed.**

Keywords- AODV ,Black hole, Gray hole, Flooding, MANET, NS-3, , Selfish Node, SVM.

I. INTRODUCTION

Mobile Ad hoc networks have paying attention of researchers and diligence due to its intrinsic ease and enormous possibility. Though, various inherent possessions ad- hoc networks [1] [2] such as infrastructure less, the absence of trusted centralized nodes, and mobility make them extremely vulnerable to various types of attacks, making security a critical issue for such networks.

Wireless networks allow hosts to travel without the constraints of wired connections. Hosts and routers in a wireless network can move around. Therefore, the network topology can be dynamic and unpredictable. A MANET uses multi-hop peer-to-peer routing as an alternative of fixed network infrastructure to provide network connectivity. A Multi hop routing is used when the nodes are not in each other's radio range. Moreover, each host acts as router. Nodes have unrestricted mobility and connectivity that causes frequently changes in network topology. There are no permanent routers- instead each node acts as router and frontwards traffic from other nodes. Due to highly dynamic nature topology in MANET makes routing procedure more complicated and insecure and therefore nodes are more susceptible to compromise and are particularly vulnerable to denial of service attack (DoS) attacks launched by malicious nodes or intruders [3].

In modern age of communication security is main concerns. Modern security approached is based on the concept of defense-in depth, where multiple layers of defenses are used to prevent network from misbehaving nodes. MANET is a high vulnerability Network which requires secure communication.

In this paper we have proposed a routing based method to detect selfishness of a node. Our propose method is based on AODV [4]. AODV is a well known and popular reactive type's protocol used in MANET.

Rest of the paper as organize as follow section 2 discuss Types of Attacks in MANET, section 3 gives brief literature on types of attack and exiting work related to prevention and detection, section 4 insight into our proposed work to detect flooding attack ,black hole and gray hole attack, and finally section 5 describes the conclusion of the paper.

II. ATTCKS IN MANET

Mostly MANET applied in emergency rescue operations, military and police networks, and safety critical business operations such as oil drilling platforms or mining operations need secured communications [5][6].

Today's MANET mobile ad hoc network research has paying attention to improve the performance of routing protocols and mechanism of communication in a trusted environment [1]. Authors of [7] classified MANET attacks into two categories. First one is based on the mode of attack (passive or active), and second attacks on different protocol layers. In case of passive type violations, suspicious node (intruder or attacker) does not harm network operation and acquire information silently, while in case of active mode, the attackers construct, modify or plunged network packets [7].

Another category of MANET threat classified according layering attacks. In this supervising has concentrate on the layer in which attack is launched on. For example, Network layer attackers can absorb network traffic, inject own packets into the transmission path.

In wormhole attack, an attacker records a packet at one place and tunnels them to another place where it is fabricated and retransmitted by a colluding attacker. Resulting, distant nodes receive distorted route information of topology and feels themselves as direct neighbors. This type of attacks

might be launched even if the network offers confidentiality [2].

Abderrahmane Baadache and Ali Belmehdi [8] address the importance of security in MANET. According to authors [8] securing of MANET is make sure mutual authentication of participants nodes, confidentiality and integrity of exchanged data, availability of the network resources, access control to the communication medium and the anonymity.

According to Authors of [9] [10] MANET attacks generally includes attempting to drop or modify packets, gaining authentication or procuring authorization by inserting false packets into data stream [11].

Various types of attacks has been identified [11] some of them are – (i) Denial of Service Attack (DoS) [12] (ii) The Flooding Attack is a special type of denial-of-service attack in which malicious nodes which malicious node sends the useless packets to consume the valuable network resources. Flooding attack is possible in all most all on demand routing protocol [13][14]. (iii) Attacks to overflow the Routing table (iv) Impersonation (v) Power consumption (vi) Information disclosure (vii) Packet modifying (viii) Selfish Node - Selfish nodes are those which save their resources by not taking part in communication. (ix) Black hole [15] [16] (x) Gray Hole [17][18] [19] (xi) Worm Hole [20].

Many methods has been proposed to solve the wormhole detection and prevention author of [21] has review and addresses a technique based on a variant of the counting technique [22] in which nodes broadcast group of hashes of the packets received out of last k time intervals.

The method proposed by the author of [22] uses signature and timestamp schemes to check authentication and protection against replay attacks. Signature based techniques uses a signature with each routing control packets as in [23].

III. LITERATURE SURVEY

Primarily Statistical analysis has been used to detect malicious node who floods in the network using RREQ messages, [24] has proposed a statistical approach to avoid the forwarding of such packets using the concept of RREQ counts.

Author Bo-Cang Peng and Chiu-Kuo Liang of [25] has suggested the concept of friendship table for detection of intrusion on MANET. Friendship table is used to store the relationship status of any node with its neighbors. The friendship table has two columns. First the identifier or name of its entire neighboring node and second its relationship status with the neighbor node that could be friend, Acquaintance or stranger. This table is referred every time when any node receives the packets. Initially NODE treat as stranger while newly joined the network. If the trust value is optimal node will treat as acquaintance, If node receives many packets to or from any node successfully, then trust level is very high the node is considered as a friend.

In [26][27][28] has used the concept of dynamic routing metrics like RREQ , RREP and the idea of route freshness calculated using destination sequence number for detection and prevention of flooding and black hole attacks of MANET.

The author Fan-Hsun Tseng, Li-Der Chou1 and Han-Chieh Chao of [29] has experience that a higher packet delivery ratio is obtained with only minimal delay and overhead. But the end-to-end delay might be raised visibly when the suspicious node is away from the source node The experiment have been performed using global mobile simulator (GloMoSim).

Time-based Threshold Detection Scheme [30] Latha Tamilselvan et al. propose a solution based on an enhancement of the original AODV routing protocol. The major design concept is setting timer in the Timer Expired Table for collecting the other request from other nodes after receiving the first request. It will store the packet's sequence number and the received time in a Collect Route Reply Table (CRRT), counting the timeout value based on the arriving time of the first route request, judging the route belong to valid or not based on the above threshold value.

Author Tamilselvan L, Sankaranarayanan [30] has used to concept of feedback to detect cooperative black holes, the node that ultimately eats up the data packets gets trapped. Moreover, Source Node decides the location of a black hole by the feedback of more than one neighboring node. Hence the detection and elimination of malicious node has been possible.

Sun et al [31] presented a general approach for detecting the black hole attack. They devised a neighborhood-based technique to detect the intruder and a routing recovery protocol to set up an accurate path to the true destination. One drawback of this scheme is that there must be a public key infrastructure or the detection is still susceptible.

Patcha et al [32] proposed a collaborative method for black hole attack prevention. A watchdog method is introduced to incorporate a collaborative architecture to tackle collusion amongst nodes. In this algorithm, nodes in the network are classified into trusted, watchdog, and ordinary nodes. Every watchdog that is elected should observe its normal node neighbors and decide whether they can be treated as trusted or malicious.

Gao et al [33] proposed to use aggregate signature algorithm to trace packet dropping nodes. The proposal was consisted of three related algorithms: 1) the creating proof algorithm. 2) The checkup algorithm. 3) The diagnosis algorithm.

Shila et al [34] presented a solution to defend selective forwarding attack (gray hole attack) in Wireless Mesh Networks. The first phase of the algorithm is Counter-Threshold Based and uses the detection threshold and packet counter to identify the attacks. The second phase is Query-Based and uses acknowledgment from the intermediate nodes to localize the attacker.

Author D.S.J.D. Couto; D. Aguayo; J. Bicket; R. Morris of [35]has proposed has based on detect black and gray hole nodes, the sender occasionally check through all available routes to determine if the destination received all of its messages undamaged. In order to circumvent any black hole nodes that might interfere with message traffic, the sender

broadcasts a "check" request message and the destination's response would follow the same route as the request.

Some researchers also discussed and proposed a solution to a black hole attack by disabling the ability for intermediate nodes to reply to an RREP, and only allowing the destination to reply.

Payal N. Raj, Prashant B. Swadas [36] proposed DPRAODV (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The RREP is accepted if its sequence is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value, if it is higher than threshold value than it is considered as the malicious node. The value of the threshold value is dynamically updated in the time interval.

Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard [37] proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets. The Route request (RREQ) is sent by source to every node and it send packet to the node from where it get the RREP. The intermediate node should send NHN and the DRI entry to the table. The source node (SN) check own DRI whether intermediate node (IN) node is reliable or not. The SN send the further request to next hop node (NHN) for IN. If SN uses IN to send the packet then it is considered as reliable node otherwise not. Cross checking is done on the intermediate nodes. It is one time procedure. The cost of cross checking is more. It can be minimized by letting nodes sharing their trusted nodes list with each other.

Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park [38] proposed two different approaches to solve the black hole attack. The first solution the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the redundancy of the network. The idea of this solution is to find more than one route for the destination. The SN unicast the ping packet using different routes. The IN or destination node or malicious node will ping requests. The SN checks the acknowledgment and processes them to check which one is safe or having malicious node. In the meantime the SN buffered its packet until it found the safe route. When the route is identified the buffered packets will be transmitted to it. The drawback of the solution is the time delay. The second solution is to store the last sent packet sequence number and the last received packet sequence number in the table. It is updated when any packet is arrived or transmitted. When node receives reply from another node it checks the last sent and received sequence number. If there is any mismatch then an ALARM indicates the existence of a black hole node. This method is faster and more reliable and has no overhead.

Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng, and Shun Chao Chang [39] proposed a distributed and cooperative procedure to detect black hole node. In this each node detect local anomalies. It collects information to construct an estimation table which is maintained by each node containing information regarding nodes within power range. This scheme is initiated by the initial detection node which first broadcast and then it notifies all one-hop neighbors of the possible suspicious node. They cooperatively decide that the node is suspicious node. Immediately after the conformation of black hole, the global reaction is activated to establish proper notification system to send warning to the whole network. The simulation result show the higher black hole detection rate and achieves better packet delivery. When the network is busier it achieves less overhead.

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto [40] use an anomaly detection scheme. It uses dynamic training method in which the training data is updated at regular time intervals. Multidimensional feature vector is defined to express state of the network at each node. Each dimension is counted on every time slot. It uses destination sequence number to detect attack. The feature vector include Number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. They calculate mean vector by calculating some mathematical calculation. They compare distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack. The updated data set to be used for next detection. Repeating this for time interval T anomaly detection is performed.

Hongmei Deng, Wei Li, and Dharma P. Agrawal [41] proposed a solution for single blackhole node detection. In this method, each intermediate node is used to send backs the next hop information when it sends back an RREP message. After getting the reply message, the source node does not send the data packets but extracts the next hop information from the reply packet and then it sends a Further- Request to the next hop to verify that it has a route to the intermediate node who sends back the Further reply message, and that it has a route to the destination node.

Hesiri Weerasinghe [42] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the Ramaswamy to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). The simulation result shows that the AODV and the solution proposed by Deng et al. highly suffer from cooperative black hole in terms of throughput and packet losses. The performance of the solution is good and having better throughput and minimum packet loss percentage over other solutions.

Many secure routing methods have been proposed to achieve routing security and providing safe guard attackers

to modifying the packets (data) or contaminate routing messages into the network [43] [44] [45] [46] [47].

Author of [44] address two types of node which perform routing misbehavior into Type 1 and Type 2. Type1 nodes behave nicely as per the routing mechanism including route discovery, maintenance, and packet forwarding and receiving whereas Type 2 nodes are do nothing with the packet sent to it; thus action has been performed i.e. they acted as a selfish node (or selfish behavior) to accumulate the battery power. They have been worked as a resting node within the network, since they impede contribution to the network maintenance, routing discovery, packet forwarding and receiving.

Author of [48] focused on attack launched by intermediate node whose drops packets passing through it. The objective of the dropper node is too preserved resources, such as battery power. These types of node called selfish node.

A denial of service (DoS) attack is used to destruct the end-to-end communication [9] by attacker nodes. These types of nodes is called malicious node. To accomplish this type of attack, the dropper node must be in the communication path between the source and the destination nodes, and afterward it starts drop packets passing through it.

To detect suspicious (dropper) node author [48] proposed a scheme based on Merkle tree [49]. The authors proposed idea was, Suppose, A, B and C be three nodes which after route establishment. The node A holds the value a1 pre-calculated from values a (owned by A), b1 owned by B and c1 owned by C. The acknowledgment of the sent message from A through B , the node C sends back its value to B, and B sends back the received value cl plus b1 to A. When A receives b1 and c1, it recalculates a1 from a (his own value), b1 and c1. If the recalculated value a1 is same already held, so message was well delivered by node B, else B is a possible dropper node.

Sharma and Gupta [50] observed that packet dropping attack has a pessimistic impact on the MANET functioning. Authors [50] evaluated an AODV-based network performance, in the presence of suspicious nodes, is reduced up to 26%. Marti et al. [51] found that if 10–40% of nodes misbehave during packets forwarding, network average throughput degrades by 16–32%. For demonstrating that an effective protection against selfish and malicious nodes is absolutely mandatory for ad hoc networks,

Kargl et al. [52] observed the MANET performance under a varying number of selfish nodes obtained statistics proved that, selfish nodes has create a negative impact on packet delivery ratio (PDR) in the network. Same results found by Buttya and Hubaux [53].

Jian Wang et al. [54] focused on the necessity of routing security, author concludes the general theory about MANET routing protocols is that all the nodes are reliable and cooperative nature [55], i.e., all the nodes behave as per the protocol specifications. However, the assumption is wrong due to malicious behaviors among nodes. For example selfish nodes refuse relaying of packets coming from other nodes, and disturb the network by malicious nodes. Few attacks like man-in-the-middle, black hole, gray hole, and Denial of Service (DoS), targeted to ad-hoc network.

Author [54] study focused on trust scheme in MANET routing for enhancing of security among nodes. The perception of trust in distributed computer networks is consequent of social science. According to Luo [56], trust is the firm conviction in the fitness of an object to act dependably, securely and reliably within a specific circumstance. Authors of [57] classify trust into two types, identity and behavioral. Identity trust is to verifying the authenticity of an individual, while behavioral trust deals with a broader view of the trustworthiness of an entity depending on the circumstances.

Author [54] has proposed a new scheme to secure routing for MANET. Authors proposed solution summarized in following steps: (1) they proposed a novel scheme for evaluation of trust among nodes using attribute similarity (2) Method for computing the attribute similarity between pair of nodes.

Yau and Mitchell [58] categorized MANET internal attacks failed, badly failed, selfish and malicious nodes [59]. Author [59] proposed a trust based mechanism to detect and prevent selfishness behavior of a node based on game theory.

According to Buttyan and Hubaux [60], a selfish node is one who only wants to benefit from other nodes although decline to share its own resources [61].

IV. PROPOSED METHODOLOGY

Our proposed solution is influenced from [63], Author proposed threshold based technique to detect the behavior of selfish node. To enhance the performance of the above mentioned scheme we have integrated the idea of classification of the behavior of Selfishness using support vector machine proposed by [65].

According to the [63] nodes are planned to expand the maximum reimbursement from the networks even as safeguard their own resources like hardware, battery power or bandwidth. Selfish nodes do only outgoing from their own. Hence they only send data packets to other node as a source. While after receiving packets from other nodes they refused to cooperate. Consequently, they start dropping of packets or refuse.

Authors of [64] outline the possible behaviors of the selfish node in AODV-

1) *Do not forward RREQ messages*
2) *Do not send Hello messages.*
3) *Do not forward Data message.*
4) *Delayed forwarding RREQ messages.*
5) *Do not forward RREP messages.*

The following proposed methodology we have develop to restrict the selfishness of a node in wireless infrastructure less environment –

1. Captureing/recording the behavior of each node (using ***packet delivery, modification and route modification ratio*** of a node).
2. Applying the threshold mechanism on each node to restrict the flooding of unnecessary route control packets in the network (Using monitoring pr

supervision of behavior) with help of support vector machine (SVM).

The proposed methodology will be tested under NS-3.13 [62] on UBUNTU environment.

.

V. CONCLUSION

In this article we have discuss various types of attack that have been worked as weapon for intruders to disrupt the communication in MANET. Literature survey concludes that most of the attacks are launch during route discovery such as Flooding, Black Hole and Gray Hole and selfish the dangerous one. In this paper we have presented a descriptive work and study on wireless security has been done till date. Finally this article proposed a methodology to detect and restrict the selfishness of a node. Proposed methodology has work efficiently due to its simplicity as our experiments summarize. The evaluation of the methodology will be presented soon in the next series of this paper.

REFERENCES

[1] P. Brutch, C. Ko, Challenges in intrusion detection for wireless ad-hoc networks, in: Proceedings of the 2003 Symposium on Applications and the Internet Workshops, 2003.

[2] John Felix Charles Joseph, Amitabha Das, Boon-Chong Seet, Bu-Sung Lee "Opening the Pandora's Box: Exploring the fundamental limitations of designing intrusion detection for MANET routing attack", Elsevier Computer Communications 31 (2008) 3178–318. Available at ScienceDirect.

[3] Basangi, S., Conti, M., Giordano, S. and Stojmenovic, I. 2004. Mobile ad hoc networking. IEEE Press. Wiley-Interscience. P-282.

[4] Alokparna Bandyopadhyay, Satyanarayana Vuppala and Prasenjit Choudhury "IEEE, Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2nd International Conference,2011

[5] Mohammad Rafiqul Alam and King Sun Chan "RTT-TC: A Topological Comparison Based Method to Detect Wormhole Attacks in MANET", IEEE, 2010.

[6] Z. Tun and A. H. Maw, "Wormhole attack detection in wireless sensor networks," in Proceedings of World Academy of Science, Engineering and Technology, vol. 36, 2008.

[7] F. Nait-Abdesselam, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," IEEE Commun. Mag., vol. 46, no. 4, pp. 127-133, Apr. 2008.

[8] C.E. Perkins, and E.M. Royer, Ad-hoc On-demand Distance Vector Routing, in: Proceedings of the 2th IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp.90-100.

[9] Abderrahmane Baadache and Ali Belmehdi "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks", Elsevier Journal of Network and Computer Applications 35 (2012) 1130–1139. Availavle at SciVerse ScienceDirect.

[10] V. Karpijoki, Security in ad hoc networks. in: Proceedings of the Helsinki University of Technology, Seminars on Network Security ,2000.

[11] J. Lundberg, Routing security in ad hoc networks, in: Proceedings of the Helsinki University of Technology, http://citeseer.nj.nec.com/400961.html.

[12] Jung-Shian Li and Cheng-Ta Lee "Improve routing trust with promiscuous listening routing security algorithm in mobile ad hoc networks", Elsevier Computer Communications 29 (2006) 1121–1132. Available at science direct.

[13] P. Papadimitratos, Z.J. Haas, Secure routing for mobile ad hoc networks, SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[14] Alokparna Bandyopadhyay1, Satyanarayana Vuppala, Prasenjit Choudhury, "A Simulation Analysis of Flooding Attack in MANET using NS-3", 978-1-4577-0787-2/11/$26.00 ©2011 IEEE

[15] A.Vani, D.Sreenivasa Rao, "Providing of Secure Routing against Attacks in MANETs",International Journal of Computer Applications (0975 – 8887) Volume 24– No.8, June 2011

[16] Raja Karpaga Brinda .R, Chandrasekar.P , " Detection and Removal of Co-Operative Black Hole\Black Hole Attack in Manet", International Journal of Computer Applications (0975 – 8887) Volume 43– No.11, April 2012

[17] Madhusudhananagakumar KS , G. Aghila, "A Survey on Black Hole Attacks on AODV Protocol in MANET" , International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011

[18] Vishnu K, and Amos J .Paul," Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks." International Journal of Computer Applications 2010, Volume 1-No.22, pp.38-42.

[19] Onkar V.Chandure, V.T.Gaikwad, " Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", International Journal of Computer Applications (0975 – 8887) Volume 41– No.5, March 2012

[20] Mahendra Kumar, Ajay Bhushan, Amit Kumar," International Journal of Advanced Research in Computer Science and Software Engineering", Volume 2, Issue 4, April 2012

[21] 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, 2009

[22] C. Adjih, T. Clausen, A. Laouiti, P. M ¨uhlethaler, and D. Raffo,"Securing the OLSR routing protocol with or without compromised nodes in the network," HIPERCOM Project, INRIA Rocquencourt, Tech. Rep. INRIA RR-5494, February 2005.

[23] D. Raffo, C. Adjih, T. Clausen, and P. M ¨uhlethaler, "An advanced signature system for OLSR," in SASN '04: Proceedings of the 2nd ACM Workshop on security of ad hoc and sensor networks. New York, NY, USA: ACM Press, 2004, pp. 10–16.

[24] S. Kannan, T. Kalaikumaran, S. Karthik and V.P. Arunachalam,"A Review on Attack Prevention Methods in MANET" Journal of Modern Mathematics and Statistics Year: 2011 | Volume: 5 | Issue: 1 | Page No.: 37-42

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

[26] Harsh Pratap Singh, Sanjeev Sharma "Guard against cooperative black hole attack in Mobile Ad-Hoc Network" Harsh Pratap Singh et al. / International Journal of Engineering Science and Technology (IJEST)

[27] Lalit Himral, Vishal Vig & Nagesh Chand, "Preventing AODV Routing Protocol from Black Hole Attack" Lalit Himral et al. / International Journal of Engineering Science and Technology (IJEST)

[28] Rajib Das,Dr. Bipul Syam Purkayastha, Dr. Prodipto Das "Security Measures for Black Hole Attack in MANET: An Approach "Rajib Das et al. / International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462 Vol. 3 No. 4 Apr 2011.

[29] Fan-Hsun Tseng, Li-Der Chou1 and Han-Chieh Chao,"A survey of black hole attacks in wireless mobile ad hoc networks "Tseng et al. Human-centric Computing and Information Sciences 2011, 1:4

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

[31] Greece, June 2006.B. Sun; Y. Guan; J. Chen; U.W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks" 5th European Personal Mobile Communications Conference, 2003, 490-495.

[32] A. Patcha; A. Mishra; "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks" Radio and Wireless Conference, 2003, 75-78.

[33] X.P. Gao; 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.

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

[35] D.S.J.D. Couto; D. Aguayo; J. Bicket; R. Morris, "A High-Throughput Path Metric for Multi-Hop Wireless routing," in ACM Mobicom, 2003.

[36] 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, 2009

[37] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks"

[38] Mohammad Al-Shurman and Seong-Moo Yoon and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks"

[39] Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng, and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 Workshops, pp. 538–549, 2007

[40] 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, Issue 3, pp: 338–346, 2007

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

[42] Hesiri Weerasinghe, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, vol. 02, pp: 362-367, 2007

[43] Yogesh Sharma and Sunil Kumar "Effect of Power Avaricious Attack on MANET Routing Protocols", IEEE, 2011.

[44] H. Li and M. Singhal. A secure routing protocol for wireless adhoc networks. In HICSS'06: Proceedings of the 39th Annual Hawaii International Conference on System Sciences. Pages 1-10, 2006.

[45] Hongmei Deng, Wei. Li and Dharma P. Aggarwal. Routing Security in Wireless Adhoc Networks. In IEEE communication magazine, Pages 70-75, October-2002.

[46] K. Paul and D. Westhoff. Context aware detection of selfish nodes in DSR based adhoc networks. In IEEE GLOBECOM 2002, Taipei, Taiwan, pages 178-182, November 2002.

[47] P. Papadimitratos and Z.J. Haas. Securing routing for mobile adhoc networks. In Proceedings of SCS communication networks and distributed systems modeling and simulation conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

[48] Abderrahmane Baadache and, Ali Belmehdi "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks", Elsevier, Journal of Network and Computer Applications 35 (2012) 1130–113.

[49] Buchmann J, Dahmen E, Schneider M. Merkle tree traversal revisited. In: Proceedings of the 2nd international workshop on post-quantum cryptography (PQCrypto'08); 2008. p. 63–78.

[50] Sharma S, Gupta R. Simulation study of blackhole attack in the mobile ad hoc networks. Journal of Engineering Science and Technology 2009;4(2):243–50.

[51] Marti S, Giuli TJ, Kevin L, Mary B. Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th annual international conference on mobile computing and networking (MobiCom'00); 2000. p. 255–65.

[52] Kargl F, Klenk A, Schlott S, Weber M. Advanced detection of selfish or malicious nodes in ad hoc networks. In: Proceedings of the 1st European on security in ad-hoc and sensor networks (ESAS'04); 2004. p. 152–65.

[53] Buttya´ n L, Hubaux JP. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applications (MONET) 2003;8(5):579–92.

[54] Jian Wang, Yanheng Liu and Yu Jiao "Building a trusted route in a mobile ad hoc network considering communication reliability and path length", Elsevier, Journal of Network and Computer Applications 34 (2011) 1138–1149.

[55] Ramana KS, Chari AA and Kasiviswanth N "Trust based security routing in mobile adhoc networks", International Journal on Computer Science and Engineering 2010; 2(2):259–63.

[56] Luo J, Ni X, Yong J "A trust degree based access control in grid environments", Information Science 2009; 179(15):2618–28.

[57] Azzedin F, Maheswaran M. "Evolving and managing trust in grid computing systems", In: Proceedings of IEEE Canadian conference on electrical and computer engineering (CCECE'02); May 2002. pp. 1424–9.

[58] Yau P, Mitchell CJ "Reputation methods for routing security for mobile ad hoc networks", In: Proceedings of joint IST workshop on mobile future and symposium on trends in communications SympoTIC '03. IEEE Press; 2003. p. 130–7.

[59] K. Komathy and P. Narayanasamy "Trust-based evolutionary game model assisting AODV routing against selfishness", Elsevier, journal of Network and Computer applications, 2008.

[60] Buttyan, L., & Hubaux, J. P. "Security and cooperation in wireless networks", Cambridge University Press, 2008.

[61] Hung-Min Sun , Chiung-Hsun Chen and Yu-Fang Ku "A novel acknowledgment-based approach against collude attacks in MANET", Elsevier, Expert Systems with Applications 39 (2012) 7968–7975, 2012.

[62] NS-3 simulator, http://nsnam.org/

[63] Lien-Wen Wu and Rui-Feng Yu "A Threshold-Based Method for Selfish Nodes Detection in MANET", IEEE, 2010.

[64] S. Yokoyama, Y. Nakane, O. Takahashi, and E.Miyamoto, "Evaluation of the Impact of Selfish Nodesin Ad Hoc Networks and Detection and CountermeasureMethods," Proceedings of the 7th International Conference on Mobile Data Management (MDM 2006).

[65] Wenjia Li, Anupam Joshi and Tim Finin "SAT: an SVM-based Automated Trust Management System for Mobile Ad-hoc Networks", IEEE, Military Communications Conference, 2011 - Milcom 2011.