Volume 4, Issue 9, September 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Gray Hole Attack in MANETs

Sandeep Kumar* Dept of comp. CDLU SIRSA India
Mrs. Sangeeta Dept of comp CDLU SIRSA India
Pramod Kumar Soni Raj Rishi College Alwar India

Abstract Mobile Adhoc Networks (MANETs) are used most commonly all around the world, because it has the ability to communicate each other without any fixed network. It has the tendency to take decisions on its own that is autonomous state. MANET is generally known for infrastructure less. The bridges in the network are generally known as a base station. A unified security solution is very much needed for networks to protect both route and data forwarding operations in the network layer. Security is an essential requirement in MANET. Without any proper security solution, the malicious node in the network will act as a normal node which causes eaves dropping and selective forwarding attack generally known as Gray Hole attack. In this paper we surveyed about the different types of techniques to prevent Gray Hole Attack

Keywords— MANET, Network layer Attack, Gray Hole attack, AODV;

I. INTRODUCTION

Ad-Hoc network is called Independent Basic Service Set (IBSS) Stations. IBSS communicate with each other directly and do not have any access point. Because of the mobility of nodes in ad-hoc networks, they are commonly called MANET (Mobile Ad-hoc Network). Mobile Ad-Hoc network [1] is a group of mobile nodes which are free to move haphazardly while being able to communicate with each other without the help of an existing network infrastructure. MANETs are suitable for use in situations where any wired or wireless infrastructure is inaccessible, overloaded, damaged or destroyed such as emergency or rescue missions, disaster relief efforts and tactical battlefields, as well as civilian MANET situations, such as conferences and classrooms or in the research area like sensor networks. MANETs eliminate this dependence on a fixed network infrastructure where each station acts as an intermediate switch. Security in MANETs is a complex issue. This complexity is due to various factors like insecure wireless communication links, absence of a fixed infrastructure, node mobility, dynamic topology and resource constraints. In mobile ad hoc networks, nodes also perform the role of routers that discover and maintain routes to other nodes in the network. The primary concern of routing protocols of MANETs is to establish an efficient and optimal route between the communicating entities. Any attack can mess up overall communication and the whole network will be destroyed. Nodes are more vulnerable to security attacks in mobile ad-hoc networks than in traditional networks with a fixed infrastructure. There are different kinds of attacks by malicious nodes that can harm a network and make it unreliable for communication. One such kind of attack is gray hole attack. A gray hole attack is one in which a malicious node advertises itself as having the shortest path to a destination in a network. This can cause Denial of Service (DoS) [2] by dropping the received packets. The paper is organized as follows. Section 1 discusses the presents Security issues for MANETs. Section 3 presents about the different routing protocols used in MANET. Section 5 presents Gray Hole Attack Background and different techniques of Gray hole attack detection and prevention is discussed in section 4. Section 6 presents the conclusion and future work.

II. SECURITY ISSUES

SECURITY GOALS OF MANET

The ultimate goal for MANET is to provide security solutions. To provide a solution for security reason there are some of the mechanism which is used to prevent, detect and respond. They are mainly Availability, Confidentiality, Integrity and Authentication.

Availability

The network should be available only for the authenticated users and this mechanism is used to protect against the kind of attacks like Gray hole, black hole, Information disclosure and Message altering.

Confidentiality

In MANET it is very hard to attain the confidentiality due to intermediate nodes routing, which can easily retrieve the information from the routing nodes.

Integrity

The transmission of information should be protected against any alteration and message modification.

Authentication

The network should be accessed only by the authenticated nodes such as Digital signature, Reply and Non repudiation.

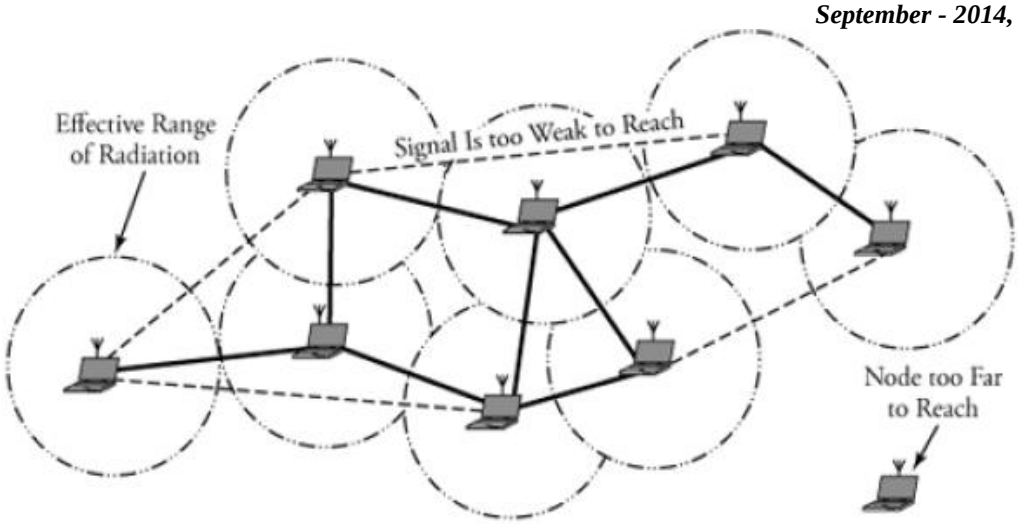

Fig. 1 Typical MANET

III. ROUTING IN MANET

The lack of a backbone infrastructure [7] coupled with the fact that mobile Ad Hoc networks change their topology frequently and without prior notice makes packet routing in ad-hoc networks a challenging task. The suggested approaches for routing can be divided into topology-based and position-based routing.

Topology-based routing protocols use the information about the links that exist in the network to perform packet forwarding. They can be further divided into *proactive*, *reactive*, and *hybrid* approaches.

Proactive algorithms employ classical routing strategies such as distance-vector routing (e.g., DSDV) or link-state routing (e.g., OLSR and TBRPF). They maintain routing information about the available paths in the network even if these paths are not currently used. The main drawback of these approaches is that the maintenance of unused paths may occupy a significant part of the available bandwidth if the topology of the network changes frequently.

In response to this observation, reactive routing protocols were developed (e.g., DSR, TORA, and AODV). Reactive routing protocols maintain only the routes that are currently n use, thereby reducing the burden on the network when only a small subset of all available routes is in use at any time. However, they still have some inherent limitations.

First, since routes are only maintained while in use, it is typically required to perform a route discovery before packets can be exchanged between communication peers. This leads to a delay for the first packet to be transmitted. Second, even though route maintenance for reactive algorithms is restricted to the routes currently in use, it may still generate a significant amount of network traffic when the topology of the network changes frequently. Finally, packets en route to the destination are likely to be lost if the route to the destination changes.

Hybrid Ad Hoc routing protocols such as ZRP combine local proactive routing and global reactive routing in order to achieve a higher level of efficiency and scalability. However, even a combination of both strategies still needs to maintain at least those network paths that are currently in use, limiting the amount of topological changes that can be tolerated within a given amount of time.

Position-based routing algorithms eliminate some of the limitations of topology-based routing by using additional information. They require that information about the physical position of the participating nodes be available. Commonly, each node determines its own position through the use of GPS or some other type of positioning service. A *location service* is used by the sender of a packet to determine the position of the destination and to include it in the packet's destination address. The routing decision at each node is then based on the destination's position contained in the packet and the position of the forwarding node's neighbors. Position-based routing thus does not require the establishment or maintenance of routes

Regardless of the approach to routing, a routing protocol should be able to automatically recover from any problem in a finite amount of time without human intervention. Conventional routing protocols are designed for nonmoving infrastructures and assume that routes are bidirectional, which is not always the case for ad-hoc networks. Identification of mobile terminals and correct routing of packets to and from each terminal while moving are certainly challenging.

Ad Hoc On-Demand Distance Vector (AODV)

AODV [15] can be thought of as a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV. AODV is an on-demand routing protocol, which initiates a route discovery process only when desired by a source node. When a source node S wants to send data packets to a destination node D but cannot find a route in its routing table, it broadcasts a Route Request (RREQ) message to its neighbors, including the last known sequence number for that destination. Its neighbors then rebroadcast the RREQ message to their neighbors if they do not have a fresh enough route to the destination node. (A fresh enough route is a valid route entry for the destination node whose associated sequence number is equal to or greater than that contained in the RREQ message.) This process continues until the RREQ message reaches the destination node or an intermediate node that has a fresh enough route. Every node has its own sequence number and RREQ ID1. AODV uses sequence numbers to guarantee that all routes are

loop-free and contain the most recent routing information. RREQ ID in conjunction with source IP address uniquely identifies a particular RREQ message. The destination node or an intermediate node only accepts the first copy of a RREQ message, and drops the duplicated copies of the same RREQ message. Each node that forwards the ROUTE REQUEST creates a *reverse route* for itself back to node S; after accepting a RREQ message, the destination or intermediate node updates its reverse route to the source node using the neighbor from which it receives the RREQ message. The reverse route will be used to send the corresponding Route Reply (RREP) message to the source node – when the ROUTE REQUEST reaches a node with a route to D, that node generates a ROUTE REPLY that contains the number of hops necessary to reach D and the sequence number for D most recently seen by the node generating the REPLY. Meanwhile, it updates the sequence number of the source node in its routing table to the maximum of the one in its routing table and the one in the RREQ message. When the source or an intermediate node receives a RREP message, it updates its *forward route* to the destination node using the neighbor from which it receives the RREP message. It also updates the sequence number of the destination node in its routing table to the maximum of the one in its routing table and the one in the RREP message. A Route Reply

Acknowledgement (RREP-ACK) message is used to acknowledge receipt of a RREP message. The state created in each node along the path from S to D is hop-by-hop state; that is, each node remembers only the next hop and not the entire route, as would be done in source routing.

IV. GRAY HOLE ATTACK

Since MANET is multihop in nature, it sturdily depends upon the cooperation among the nodes in the network [3]. The guarantee of cooperation among nodes is required. In recent times we have seen a variety of attacks have been identified and detected in the network. To provide a secure communication in the network we need to face the security challenges [6]. There are two major categories where we have to consider always in the security attacks, they are Passive attacks and Active attacks. A passive attack won't interrupt the normal operation of MANET, while data have been exchanged from the network. The solely nature of passive attack is to identify the data exchanged in the network The attacker snoops the data exchanged in the network without altering it. Here the requirements of confidentially gets violated. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for the attacker to get useful information from the data overhead.

An Active attack always tries to modify the normal operation of MANET, which means the interruption have been made in the network, such as doing data interruption, modification, deletion and fabrication. Active attacks can be internal or external. The information which is routing through -the nodes in MANET is altered by an attacker node. Attacker node also streams some false information in the network. Attacker node also do the task of route request though it is not authenticated node so the other node rejecting its request due to these route requests the bandwidth is consumed and network is jammed Some of the security threats in the networks are Interruption, Interception and Modification. In *External attacks* the attacker aims to cause congestion in the network which can be done by propagating fake routing information or to disturb the nodes from providing services [5]. The attacker always disrupts the nodes to avail the services. In internal attack, the attacker needs to gain the access to participate in the network activities. Here the attacker comes with some malicious impersonation to get access from network as a new node.

GRAY HOLE ATTACK

A variation of black hole attack is the Gray Hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are

(a) Dropping all UDP packets while forwarding TCP packets

(b) Dropping 50% of the packets or dropping them with a probabilistic distribution.

These are the attacks that seek to disrupt the network without being detected by the security measures. Gray Hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node [9]. If a source node is in need to route a packet to the destination node it uses a specific route and it will be checked in the routing table whether it is available or not. If a node initiates a route discovery process by broadcasting

Route Request (RREQ) message to its neighbour; by receiving the route request message the intermediate nodes will update their routing tables for reverse route to the source [10]. A route reply message is sent back to the source node when the RREQ query reaches either to the destination node or to any other node which has a current route to destination.

The Gray Hole attack has two phases:

Phase 1:

A malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intention of interrupting packets of spurious route.

Phase 2:

In this phase, the nodes has been dropped the interrupted packets with a certain probability and the detection of Gray Hole attack is a difficult process. Normally in the Gray Hole attacks the attacker behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [8]. Both normal node and attacker are same. Due to this behavior it is very hard to find out in the network to figure out such kind of attack. The other name for Gray Hole attack is node misbehaving attack.

V. TECHNIQUES OF GRAY HOLE ATTACK DETECTION AND PREVENTION

5.1. Neighborhood-based and Routing Recovery Scheme

Sun B et al. use AODV as their routing protocol and simulation is done in ns2 simulator. The detection scheme used neighborhood-based method to detect the black hole/gray hole attack and then present a routing recovery protocol to build the true path to the destination. Based on the neighbor set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two major steps are: Step 1-Collect neighbor set information. Step 2-Determine whether there exists a black hole/gray hole attack. In Response procedure, Source node sends a modify-Route-Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination. This scheme effectively and efficiently detects black hole/gray hole attack without introducing much routing control overhead to the network. Simulation data shows that the packet throughput can be improved by at least 15% and the false positive probability is usually less than 1.7%. The demerit of this scheme is that it becomes useless when the attacker agrees to forge the fake reply packets. This technique published in year 2003 and the simulation is done in NS-2 simulator.

5.2. Using watchdog/pathrater Scheme:

S. Marti, T. J. Giuli, K. Lai, and M. Baker (2000) proposed to trace malicious nodes by using watchdog/pathrater. In watchdog when a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet by promiscuously listening to the next node's transmissions. If the watchdog finds the next node does not forward the packet during a predefined threshold time, the watchdog will accuse the next node as a malicious node to the source node; The proposal has two shortcomings: 1) to monitor the behavior of nodes two or more hops away, one node has to trust the information from other nodes, which introduces the vulnerability that good nodes may be bypassed by malicious accusation; 2) The *watchdog* cannot differentiate the misbehavior from the ambiguous collisions, receiver collisions, controlled transmission power, collusion, false misbehavior and partial dropping. In *pathrater* algorithm each node uses the *watchdog's* monitored results to rate its one-hop neighbors. Further the nodes exchange their ratings, so that the *pathrater* can rate the paths and choose a path with highest rating for routing. Shortcoming of this algorithm is that the idea of exchanging ratings genuinely opens door for blackmail attack.

5.3.Counter- Threshold Based & Query- Based Scheme

D.M. Shila; T. Anjali (2008) offered a solution to defend selective forwarding attack (gray hole attack) in Wireless Mesh Networks. The first stage of the algorithm is Counter- Threshold Based and uses the detection threshold and packet counter to discover the attacks. The second stage is Query- Based and uses acknowledgment from the intermediate nodes to confine the attacker. In the first stage, two types of packets, Control packet and Control ACK packet, are used to detect the attacker. Furthermore, they determine the proper value of detection threshold based on the routing Expected Transmission Count metric ETX to improve the performance under different network situation.

5.4 Aggregate signature algorithm

Gao Xiaopeng, Chen Wei (2007) 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. The strengths of this suggestion are: (1) the reliability is satisfying, as proof on forwarded packets is used; (2) the application scope is wide, as bidirectional communication links are not necessary; (3) the security is satisfying, as it is hard for malicious nodes to flee detection; (4) the bandwidth overhead is low, as nodes do not need to check each other.

5.5 Centralized intrusion detection scheme based on Support Vector Machines

Sophia Kaplantzis, Alistair Shilton, Nallasamy Mani, Y. Ahmet S and Ekercio Glu (2007) presented a centralized intrusion detection scheme based on Support Vector Machines (SVMs) and sliding windows. This system can detect black hole attacks and selective forwarding attacks with high accuracy without depleting the nodes of their energy. They focus on adapting a simple classification based IDS to detect a specific spectrum of malicious DoS attacks, namely the Selective Forwarding Attack, that may be launched against a WSN. This IDS uses routing information local to the base station of the network and raises alarms based on the 2D feature vector (bandwidth, hop count). Classification of the data patterns is performed using a one-class SVM classifier. Support vector machines (SVMs) are a class of machine learning algorithms, due originally to Vapnik. While originally formulated for binary classification, they have since been extended to include regression, density estimation, and one-class classification. Over the last decade, SVMs have gained popularity due to their ability to tackle complex highly nonlinear problems in a consistent structured manner, while simultaneously avoiding problems of over fitting on simpler problem

5.6. Cross layer intrusion detection architecture based scheme

Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han (2010) proposed a novel cross layer intrusion detection architecture to discover the malicious nodes and different types of DoS attacks by exploiting the information available across different layers of protocol stack in order to improve the accuracy of detection. They used cooperative anomaly intrusion detection with data mining technique to enhance the proposed architecture. This architecture also detect sink hole attack at different layers of the protocol stack and detect various types of UDP flooding attack in an efficient way.

5.7. Channel appraised method

Vigilkumar V V, V. Mary Anita Rajam (2012) proposed a channel appraised method to detect colluding selective forwarding attack is considered. The detection is done in two phases. In the first phase, the channel estimation is integrated with traffic monitoring to achieve detection of selective forwarding attack, which can effectively identify selective forwarding misbehavior hidden in the normal loss events due to bad channel quality or medium access collisions. In the second phase, it integrate colluding node detection scheme with detection of individual selective forwarding attack.

5.8. TWOACK scheme

K. Balakrishnan, D. Jing and V. K. Varshney (2005) proposed a TWOACK scheme which can be implemented as an add-on to any source routing protocol. Instead of detecting particular misbehaving node, TWOACK scheme detects misbehaving link and then seeks to alleviate the problem of routing misbehavior by notifying the routing protocol to avoid them in future routes. It is done by sending back a TWOACK packet on successful reception of every data packet, which is assigned a fixed route of two hops in the direction opposite to that of data packets. Basic drawback of this scheme includes it cannot distinguish exactly which particular node is misbehaving node. Sometime well behaving nodes became part of misbehaving link and therefore can not be further used the network. Thus a lot of well behaved node may be avoided by network which results in losing of well behaved routes

5.9. Two-fold approach

Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema, and Attique Ahmed (2008) proposed a two-fold approach for detection and isolation of nodes that drops data packets. First approach attempts to detect the misbehavior of nodes and will identify the malicious activity in network. It is done by sending an ACK packet by each intermediate node to its source node for confirming the successful reception of data packets. If the source node does not get ACK packet by intermediate nodes then source node send again its packet for destination after a specific time. If same activity was observed again then source node broadcast a packet to declare the malicious activity in the network. Other approach identifies exactly which intermediate node is doing malicious activity. It is done by monitoring the intermediate nodes of active route by the nodes near to active path which lies in their transmission range and by the nodes which are on the active route.

5.10 Adaptive approach based on a cross layer design

Jiwen Cai, Ping YI, Jialin Chen, Zhiyang Wang and Ning Liu (2010) proposed a method to detect black hole and gray hole in wireless ad-hoc network using an adaptive approach based on a cross layer design. In this paper, a path based method was used to overhear the next hop's action. In MAC layer, a collision rate reporting system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. The average detection rate is above 90% and the false positive rate is below 10%. After analyzing the merits and demerits of the above method, they proposed dynamic threshold and adaptive detection method to enhance the detection performance

VI. CONCLUSION AND FUTURE WORK

A Gray Hole attack is one of the serious security problems in MANETs. It is an attack where a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper a survey on different existing techniques for detection of gray hole attacks in MANETs with there defects is presented. The detection techniques which make use of proactive routing protocol have better packet delivery ratio and correct detection probability, but have higher overheads. The detection techniques which make use of reactive routing protocols have low overheads, but have high packet loss problem. Therefore, we suggest having a hybrid detection technique which combines the advantages of both reactive and proactive routing for future research direction. Although these may not be avoided in totality, there is a need for trade-offs to achieve a secure optimal performances. Based on the above performance comparisons, it can be concluded that Gray Hole attacks affect network negatively. Hence, there is need for perfect detection and elimination mechanisms. The detection of Gray Holes in ad hoc networks is still considered to be a challenging task. Future work is intended to an efficient Gray Hole attack detection and elimination algorithm with minimum delay and overheads that can be adapted for ad hoc networks susceptible to Gray Hole attacks.

REFERENCES

[1] P. Agrawal, R.K Ghosh, S.K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks", ICUIMC'08.

[2] Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks " Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, " Mitigating Routing Misbehavior in Mobile Ad Hoc Networks." *Proceedings of the 6th annual international conference on Mobile Computing and Networking (MOBICOM)*, Boston, Massachusetts, United States, 2000, 255-265.

[4] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-organized network-layer security in mobile ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 24, issue 2, pp. 261-273, February 2006.

[5] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. "Prevention of cooperative black hole attack in wireless ad hoc networks." In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), pages 570–575. Las Vegas, Nevada, USA, 2003

[6] Oscar F. Gonzalez, Michael Howarth, and George Pavlou, Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks. Center for Communications Systems Research, University of Surrey, Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.

[7] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method" International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 1, January 2012)

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

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

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

[11] Gao Xiaopeng, Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", IFIP International Conference on Network and Parallel Computing Workshops 2007, pp. 209 -214.

[12] Xie Lei, Xu Yong-jun, Pan Yong and Zhu Yue-Fei. "A Polynomial-based Countermeasure to Selective Forwarding Attacks in Sensor Networks" - International Conference on Communications and Mobile Computing-2009, vol. 3, pp.455-459, 2009

[13] Mukesh Tiwari, Karm Veer Arya, Rahul Choudhari and Kumar Sidharth Choudhary, "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information", Fourth International Conference on Computer Sciences and Convergence Information Technology 2009, pp 824 – 828, Nov 2009.

[14] Tran Hoang Hai, Eui-Nam Huh "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge". Seventh IEEE International Symposium on Network Computing and Applications, pp.325-331, July 2008

[15] Sophia Kaplantzis, Alistair Shilton, Nallasamy Mani, Y. Ahmet S and Ekercio Glu "Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines" Third IEEE international conference on Intelligent sensor, Sensor Networks and Information 2007, pp 335 – 340, Dec 2007sss

[16] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han. "A Novel Cross Layer Intrusion Detection System in MANET", 24th IEEE International Conference on Advanced Information Networking and Applications-2010, pp 647 – 654, April 2010.

[17] Jiwen Cai, Ping YI, Jialin Chen, Zhiyang Wang and Ning Liu, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", 24th IEEE International Conference on Advanced Information Networking and Applications-2010, pp 275-280, April 2010.

[18] Vigilkumar V V, V. Mary Anita Rajam, "Detection of Colluding Selective Forwarding Nodes in Wireless Mesh Networks Based on Channel Aware Detection Algorithm", MES Journal of Technology and Management, 2012

[19] Sonja Buchegger Jean-Yves Le Boudec, "Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks" in Proc. IEEE/ACM Workshop Mobile Ad Hoc Netw. Comput. (MobiHoc 2002), pp. 226-236, June 2002.

[20] K. Balakrishnan, D. Jing and V. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad hoc Networks," in Proc. of Wireless Communications and Networking Conference (WCNC'05), vol. 4, pp. 2137-2142, March 2005.

