A Survey on Grey Hole Attack in Wireless mesh Networks

Kanu Geete
PG. Student
Department of CSE
UIT, RGPV

Piyush Kumar Shukla
Assistant Professor
Department of CSE
UIT, RGPV

Anjana Jayant Deen
Assistant Professor
Department of CSE
UIT, RGPV

ABSTRACT

A wireless mesh network is a kind of multi-hop network and can be used as synonym for an ad-hoc network. It is a network having many to many connections with the capability of dynamically healing the network topology. Security is a challenging application of a wireless mesh network. The self configurable self organized nature makes a wireless mesh network more vulnerable to various types of attacks. Exploitation of a WMN can cause a large scale degradation of network performance. In this paper we have discussed some attacks that are performed on various layers of TCP/IP model. And we performed a comparative study for a specific network layer attack: grey hole attack. A grey hole attack is often difficult to detect and recover. There are different techniques for its detection which have their advantages and shortcomings. We have discussed some of them in this paper.

Keywords

Grey hole attack, Wireless mesh networks, Ad-hoc networks, Routing layer**.**

1. INTRODUCTION

Akyldiz [1] stated that WMNs are deployed to resolve the limitations and to improve the performance of ad hoc networks, WLANs, WPANs, and wireless metropolitan area networks. Some characteristics of a WMN are rapid deployment, self-organization and self-configuration. A mesh network contains much more connectivity than a traditional wireless network, thus it can provide better internet access in the area. WMN's can be used in many applications such as public safety, environment monitoring and across the city wireless Internet services .Mesh network contains two types of nodes, Mesh nodes and mesh clients [1]. Mesh routers have very little mobility or they can be stationary, i.e. they can be employed on rooftops to provide wireless broadband service. There are three types of wireless mesh networks Infrastructure/Backbone WMNs. Client WMNs. Hybrid WMNs. A hybrid WMN is shown in figure.1. The gateways connect a WMN to outside world (i.e. Ethernet, WiMax etc). Mesh Points (MP) having mesh functionalities provide services to mesh clients (users) (i.e. Laptop, workstations etc). Nodes having access point functionalities in addition to mesh functionalities are shown as MAP (Mesh Access Points). Some mesh functionalities are path selection and forwarding.

1.1 Security Requirements

The ultimate goal for an ad-hoc network multi hop network is to provide security solutions. There are certain mechanisms to provide security services [2] to the system. These services are mainly Availability, Confidentiality, Integrity, Authentication and non-repudiation. A brief explanation about these terms is given.

1.1.1 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.

1.1.2 Confidentiality

In an ad-hoc network it is very hard to attain the confidentiality due to intermediate nodes routing, which can easily retrieve the information from the routing nodes.

1.1.3 Integrity

The transmission of information should be protected against any deletion, modification or replay.

1.1.4 Authentication

The network should be accessed only by the authenticated nodes i.e. To assure the communicating entity is the one that it claims to be. Digital signatures can be used to provide authentication.

1.1.5 Non Repudiation

A node which sends a packet to a destination node cannot later deny that it didn't send the packet and the destination cannot deny receiving the packet.

WMN's are highly susceptible to various attacks since it relies on shared wireless medium access and limited resources malicious nodes can attack other nodes to generate useless traffic, intercept and modify packets. They can also drop the packets partially or fully to perform various attacks; black hole, grey hole, wormhole etc. Also, many other routing layer attacks are possible despite of many cryptographic security mechanisms. To achieve such type of attacks attacker may physically acquire the router to make it drop packets.

Grey hole attacks or selective forwarding attack, which we are going to study about mostly in this paper is the special case of the denial of service attacks. If a node selectively drops some packets which it has to forward along the path, it is called grey hole attack. If a node drops all of the packets which came to it, it is called a black hole attack. Attacker may simply hijack the mesh node in the WMN to launch a selective forwarding attack. Karlof *et al.* [3] first proposed selective forwarding attack and suggested a multipath forwarding approach to detect it.

.

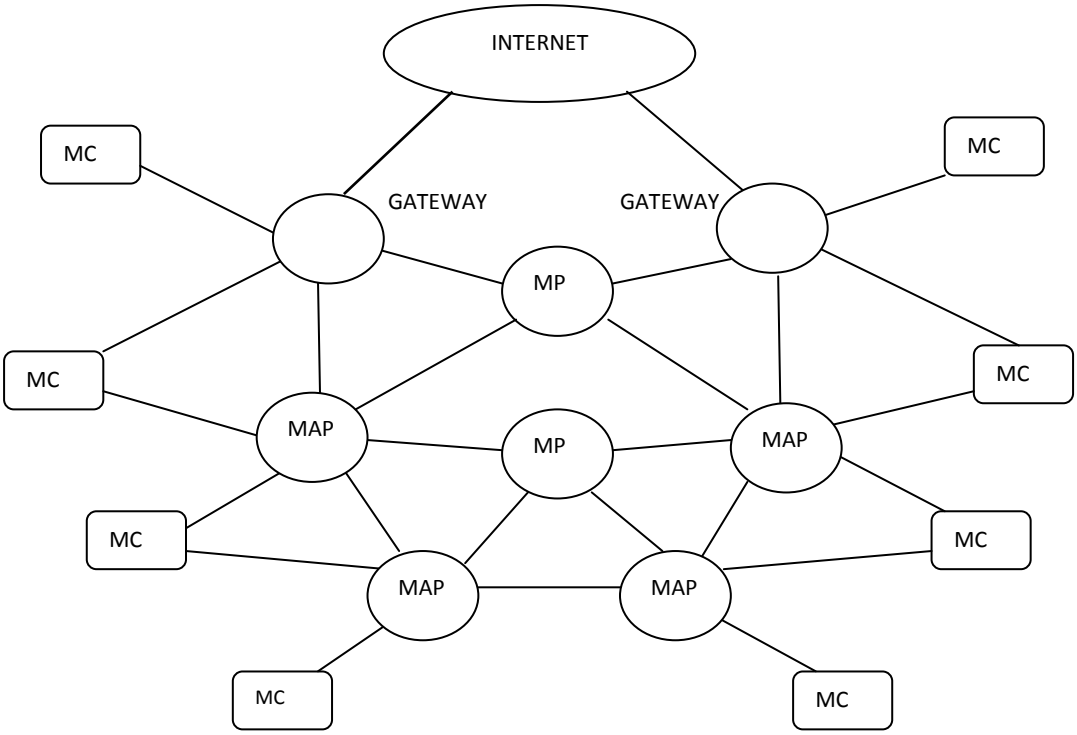

Fig 1: A Hybrid Wireless Mesh Network

2. RELATED WORKS

To mitigate selective forwarding attacks several techniques are given in previous years like MDT [4], CHEMAS [5] LEDS [6], UNMASK [7] etc. Karlof *et al.*. [3] first proposed a selective forwarding attacks and a way to detect it by using multipath forwarding technique in a sensor network. However Karlof's method didn't identifies and isolate the attackers. Same problem is with the method proposed by M. Tiwari et. al [8] and J Brown [9] for sensor networks. In [5] nodes monitor their neighborhood and collaborate with cluster head to detect malicious behavior. In [5], authors have used a technique of checkpoint selection i.e. part of intermediate nodes are selected as checkpoint nodes along a forwarding path and their job is to generate acknowledgements for each packet received. Obviously, Drawback of this method is the high overhead because of a lot of acknowledgements. In [10], Sergio Marti *et al.* have used watchdog and pathrater to detect packet dropping by a node for DSR routing protocol. A watchdog monitors its neighbor to detect any malicious behavior. The pathrater than measures the result of watchdog mechanism and selects the most reliable path for packet delivery. Methods in [4] [6] uses redundancy and [5] uses uncertainty to enhance reliability of packets delivery under selective forwarding attacks. Various attack resilient protocols Authors in [22] extended CAD to detect collaborative selective forwarding attacks. This method works in two phases, First phase detect malicious behavior using CAD, And second phase uses information gathered in first phase to detect colluding nodes. However, attackers can evade these schemes as described in FADE [23] by Liu *et al.* i.e. Two collaborating attackers can evade the detection mechanism of CAD and since Mechanism in [22] depends on CAD in its first phase Collaborating nodes can deceive it too. FADE uses a two hop acknowledgement mechanism in addition to forwarding assessment to detect colluding grey hole attack. Their scheme are given [7, 11 and 12] .A game theoretic approach is described in [13].

In [14], Authors proposed BSMR, a multicasting routing protocol which can capture colluding routing adversarial behavior. Its drawback is it uses a static detection threshold which makes it ineffective at identifying attackers at different malicious dropping rates. Certain detection methods based on traffic monitoring [15-18] where [17, 18] are capable to detect colluding grey hole nodes. Also secure routing protocols for WMN are available [8, 19 and 20].

The channel aware detection mechanism [21] considers normal packet losses due to poor channel quality or MAC layer collisions based on channel estimation and traffic monitoring to differentiate it from losses occurred due to selective forwarding attack. Channel estimation sets up a threshold by calculating normal losses and if monitored losses go beyond that threshold then those nodes are identified as malicious nodes. It can also detect Bad mouthing, On-off attack. Disadvantage with it is it cannot detect collaborative attackers.

is also capable of detecting malicious accusation, counterfeit mark attack. Results shows that FADE is able detect more sophisticated attacks and can adapt to network dynamics, such as poor channel quality and medium access collisions by adjusting detection thresholds.

In [24], Authors proposed a Secure Probabilistic routing protocol to provide secure routing against colluding insider attackers. In the first stage sprout generates routes probabilistically, focusing on diversity of routes rather than performance. In the next stage, An algorithm is used to assign

probability to every route discovered according to reliability and end-to-end delay. Probability of finding a good route increases with every new route sampled

Shila *et al.* [13] defines a framework of a non cooperative markov game between normal and malicious node. The genuine node tries to maximize the throughput by minimizing the loss caused by attackers while objective of attacker is to minimize the throughput by dropping the packets.

3. CLASSIFICATION OF ATTACKS

An important category is Active attacks and Passive attacks. In a passive attack, attacker just snoops the data exchanged in the network without altering it. Thus a passive attack never stops the normal operation of a network. Whereas, An active attacker performs modification, deletion and fabrication and hence disturbs the normal operation of a wireless network. The other major category classifies attacks into two types- External and Internal attacks. In an external attack, Attack is carried out by a node that does not belong to the network. The other one is internal attack which is more difficult to detect and carried out by an insider. Traditional cryptographic techniques are not suitable against internal compromised nodes.

Attacks can be classified according to the layer on which they work. A classification of attacks according to protocol stack is shown in Table 1. Jaydip Sen [25], Seth *et al*. [26].

Table 1. Attacks on different layers

Layers	Graphics		
Physical	Jamming, Scrambling, eavesdropping		
Data Link	Unfairness, Selfish MAC, Flooding		
Routing	Route Discovery Phase Attacks	Routing Table overflow attack, Routing Cache positioning attacks	
	Route Maintenance Phase Attacks	False routing control message	
	Data Forwarding Phase Attacks	Route Data Dropping	
	Sophisticated Attacks	Control Traffic Attacks	Rushing Attack, Flooding, Wormhole, Sinkhole, Sybil Attack
		Data Traffic Attacks	Resource Consumption Attack, Black hole, Grey hole Attack, Jellyfish, Byzantine
Transport	Syn-Flooding, De-Synchronization		
Application	Logic Errors, Buffer Overflow		

3.1 Some Network Layer Attacks

Some network layer attacks are discussed [27]

3.1.1 Black hole Attack

In Black hole attack the malicious black hole node exploits a routing protocol to advertise itself as the valid and optimal route, and then it drops all the packets which are received by it without forwarding it to the downstream node.

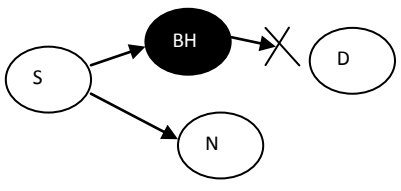

Fig 2. Black hole Attack

3.1.2 Wormhole Attack

The attacker captures packet at one location and tunnels them to another location. The tunnel thus formed is called as wormhole. It is simple for the attacker to advertise the

wormhole as a better route when the tunneled distances are longer than the normal transmission range of a single hop. I can be a serious threat to the routing protocols since it can affect the route discovery process by blocking the discovery of any route other than the wormhole. In figure 3, An extraneous link from A to B is made by intruder node X.

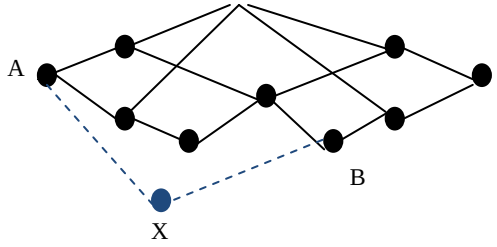

Fig. 3 Wormhole Attack

3.1.3 Grey hole Attack

Grey hole attack or selective forwarding attack is an active, data traffic, insider, routing layer attack. It can be a serious threat to data sensitive applications like health care and fire monitoring, Classified E-mails etc. A grey hole node is one which could start behaving as a black hole node from time to time i.e. It can behave like an attacker and drop the packets. So, It can be seen as a variation on black hole attack. In wireless mesh networks, The software vulnerabilities in mobile operating systems make the mesh routers more vulnerable to such attacks. However, Attacker can also make a node drop packets by physical capture since nodes can be installed on rooftops. A compromised node can drop packets silently to slowly degrade the performance of the network. Thus, detecting a grey hole attack is more complex and needs in depth studies.

The grey hole attack takes place in two phases-

- In first phase, A malicious node advertises itself as having an optimal path to the destination with the intentions of capturing the packets on that route
- In second phase, malicious node starts dropping packet on that route. After dropping some packets the node starts behaving normally again. Due to This behavior of it is difficult to detect malicious behavior in the network.

In a WMN, the network traffic aggregates at a special MR called gateway, which connects the mesh network with global network. Thus an attacker can advertise a route with minimum cost to the gateway and can selectively drop data packets received from upstream MR's. Old studies on selective forwarding attacks were performed under the assumption of error free channels [3, 5, 10 and 28]. Recent studies like CAD [21], FADE [23] also considers normal channel losses to discover presence of attacks which is more challenging task. Also, detecting a collaborative attack is more challenging than standalone attack. Studies have been carried out for standalone attacks [7, 8, 21 and 29]. Most of methods for standalone attacks based on overhearing the neighbor node's transmission and sending back the acknowledgement to upstream nodes since simplest way to detect packet losses is sending acknowledgment back to source node. However, Detecting attacks in wireless mesh network with keeping the performance high is still a problem and the tradeoff between security and overhead is still there and need to be tackled.

Table 2. Various Attack Detection Schemes

Authors	**Algorithm Name**	**Attack**	**Technique Used**	**Routing Protocol**	**Colluding/Standalone**	**Advantages**	**Drawbacks**
Liu *et al.*[23]	FADE	Grey hole, Malicious accusation, Counterfeit Mark	Forwarding Assessment and Two Hop Acknowledgement	AODV, OLSR	Colluding with two nodes	High Packet delivery Ratio, Considerable Overhead	Uses only single path Transmission, Attackers must be Two adjacent nodes
Karlof *et al.* [3]	None	Grey hole	Multipath Routing approach	All Major routing Protocols	Not specified	First theory for various attacks detection	Doesn't detect or isolate the attackers
Shila *et al.* [21]	CAD	Grey hole, Limited Transmit Power attack, On-off attack, Bad mouthing Attack	Upstream and Downstream Channel Monitoring	AODV	Standalone	High Packet Delivery Ratio, Considerable Overhead	Restricted to standalone attacker
Eriksson *et al.* [24]	Sprout	Grey hole Black hole	Probabilistic Route Generation	Sprout	Large number of colluding	High Packet Delivery ratio	Can choose polluted routes
Curtmola *et al.* [14]	BSMR	Byzintine, Insider Attacks	Reliability Metric to detect adversaries	BSMR	Colluding	High Packet Delivery ratio	Fail to detect attacks at different

							dropping rates
Sergio Marti *et al.* [10]	None	Data Packet Dropping	Watchdog and Pathrater	DSR	Standalone	Better Throughput than Standard Routing Protocols	Watchdog limitations
Hung Min Sun *et al.* [4]	MDT	Jamming, Grey hole, Sinkhole	Multi DataFlow Topologies	Not specified	Standalone	Reliability increased by introducing redundancy	Total communication distance increased due to construction of more than on topology
Issa Khalil *et al*. [7]	UNMASK	All control Traffic and Data Traffic attacks	A framework to mitigate attacks	LSR	2-4 attackers	Lightweight Protocol	Could be unsecure for mobile networks
KuiRen *et al.* [6]	LEDS	Denial Of Service Attacks	Location aware end to end data security mechanism using key management framework	Not Specific	Not specified	Provides confidentiality, authentication and High Data availability	High overhead and more consumption of resources
Bin Xiao *et al.* [5]	CHEMAS	Selective Forwarding attacks	Selecting Checkpoint nodes which generate acknowledgements	Not specified	Not specified	High Detection Rate	High overhead
Shila *et al*. [13]	None	Grey hole	Game Theoretic Approach	Not Considered	Standalone	Finds best path considering security	Assumes that only losses are due to attacks
Vigilkumar V V *et al.*[22]	None	Grey hole	Channel Aware Detection	AODV	Colluding	Extends CAD to detect colluding attacks	Sophisticated Collaborative attack can evade this
Xiaopeng & Wei[30]	None	Grey hole	Creating Proof, Checking & Diagnosis algorithms	DSR	Not specified	Reliability, Security is satisfying with low overhead	Collaborative attacks are not considered
Sen *et al*. [31]	None	Grey hole	Data Collection, Anomaly Detection, Alarming	AODV	Colluding	High detection rate with moderate overhead	Overhead increases with increase in attacking nodes
J. b. Othmen *et al.* [32]	HWMP-Watchdog	Insider Attacks	Watchdog Monitoring	HWMP	Standalone	Low Overhead	Not significant improvement in throughput
P.Agrawal *et al*. [33]	None	Black hole, Grey hole	Traffic monitoring by trusted nodes		Cooperative	Lesser Time Complexity for detection and removal of attack	Not suitable for all ad hoc networks, trusted nodes may be attackers
Kandikattu *et al.* [34]	SIMRP	Security attacks like modification, replay etc.	Framework employing Identity Based Cryptography and A secure Inter domain routing protocol	AODV	Not Specified	Security against common security attacks with less overhead	Can't perform against collaborative black hole and grey hole attack

A comparative study shows there are some good techniques to detect grey hole and other network layer attacks. A secondary goal of a technique is to increase the performance of the network with keeping the overhead low. FADE, CAD, Chemas are some of the techniques which tries to achieve both the goals. Performance of a scheme can be calculated by certain parameters. For example they are Packet Delivery Ratio, Redundancy, Reliability and throughput.

First scheme given to counter grey hole attack is by Karlof [3] using multipath routing approach. Later introduced schemes like LEDS[6] and MDT[4] did it by introducing redundancies in the network Liu et al. compared FADE with CAD and Sprout and authors in CAD compared it with Watchdog mechanism and BSMR technique on the basis of packet delivery ratio and overhead per bit. Simulation shows FADE provide better packet delivery ratio than previous techniques like CAD and sprout. Game theory approach in [4] also tries to optimize the packet delivery ratio, However, The scenario considers only simple network with the assumption that any packet loss happens only due to an attack.

4. CONCLUSION

Wireless mesh network is emerging as a useful technology to provide internet access at rural areas in a cost effective way. The inherent characteristics of a WMN like decentralization and open medium makes it vulnerable to various attacks. Thus security becomes a critical parameter for wireless mesh network. We have discussed attacks and their types in this paper on a wireless mesh network. Cryptographic schemes can be used to protect the network from external attacks. Whereas, For internal attackers we need sophisticated non cryptographic schemes. To provide complete security, non-cryptographic schemes should be used along with the cryptographic schemes. A grey hole attack is difficult to detect and remove. There are various techniques which are compared in this paper on the basis of different parameters. Previous techniques assume a standalone attacker or an error free channel for it. While considering normal losses gives a more practical solution. A survey is performed on some techniques in this paper. Also, Various security attacks are presented that can be performed on different layers.

5. REFERENCES

[1] F. Akylidz, X. Wang and W. Wang, “Wireless Mesh Networks: A Survey” Comput. Net, vol. 47 no. 4, 445-487, 2005.

[2] William Stallings, Network Security Essentials: Applications and standards, Fourth Edition, Prentice Hall, 1 Lake Street, Upper Saddle River, NJ 07458 , 2011.

[3] C. Karlof, D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures” Elsvier’s Ad Hoc J., vol 1 no. 2-3 pp 293-315 Sept 2003.

[4] H.N. Sim, C. M. CHEN and Y. C. H Asiao, “ An efficient countermeasures to the selective forwarding attack in wireless sensor networks “ in Proc. 2007 TENCON pp. 1-4.

[5] B Xiao, B. Yu, and C. Gao, “ Chemas: identifying suspect nodes in selective forwarding attacks” J. Parallel Distributed Comput. Vol 67 pp 1218-1230.

[6] K. Ren, W. Lou, Y. Jhong : LEDs : providing location aware end-to-end data security in wireless networks” IEEE Trans. Comput. ,vol. 7,no. 5, pp 585-598, 2008.

[7] I. Khalil, S. Bagchi, C. N. Rotaru and n. B. Shroff, “ Unmask: utilizing neighbour monitoring for attack mitigation in multihop wireless sensor networks” Ad Hoc Netw. Vol 8, no. 2, pp 148-164, 2010.

[8] M. Tiwari, K. V. Arya, R. Choudhary and K.S. Choudhary, “Designing intrusion to detect black hole and selective forwarding attacking in WSN based in local information” in Proc. 2009 ICCIT, pp. 824-828.

[9] J Brown and X. Du, “Detection of selective forwarding in heterogeneous sensor networks” in Proc. ICC, pp. 1583-1587.

[10] S. Marti, T. J. Giuli, K. Lai and M. Baker “ Mitigating Routing behaviour in mobile ad-hoc networks” in Proc. International conference on mobile computing and networking, Boston,Ma,200.

[11] J. Sen and A. Ukil“ A secure routing protocol for wireless sensor networks” in ICCSA 2010 ser. Lecture note in computer science Springer Berlin Heidelberg, 2010, 6018, pp. 277-190.

[12] O. Erdene-Orchir, M. Minier, F. Valois and a. Kountouris “Towards resilient routing in wireless sensor networks: gradient based routing in focus” in Proc 2010 SENSORCOMM, pp 478-483.

[13] D. M. Shila and T. Anjali, “ A Game Theoretic Approach to gray hole attacks in wireless mesh networks”, IEEE International Conference on Military communications 2008, pp. 1-7, Nov 2008

[14] R. Curtmola and C. Nita-Rotaru, “BSMR: Byzantine-resilient secure multicast routing in multi-hop wireless networks,” in Proc. Sensor, Mesh and Ad Hoc Communications and Networks, June 2007.

[15] S Misra, P.V. Krishna,K. I. Abraham, N. Sasikumar and S. Freden,” An adaptive learning routing protocol for prevention of distributed denial of service attacks in wireless mesh networks,” Comput. Mathematics Applicat.,vol 60, no. 2, pp. 294-306, 2010.

[16] J. dong, R. Curtmola and C. Neeta-Rotaru” Secure High Throughput multicast routing in wireless mesh networks” IEEE Trans. Mobile Comput.,vol. 10, no. 5,pp. 663-668,2011.

[17] W.Wang, B. Bhargava and M. Linderman, ”Defending against collaborative packet drop attacks on manets” in DNCMS2009.

[18] S.Banergee, ”Detection/Removal of cooperative black and gray hole attack in mobile ad-hoc networks” in 2008 WCECS.

[19] S. Khan and J. Loo, “Cross Layer Secure and source aware on demand routing protocol for hybrid mesh networks,” Wireless Pers. Commun. Vol. 62,no. 1,pp. 201-214, 2012.

[20] S. Khan, K.-K. Loo, N. Mast, T. Naeem, “ SRPM: Secure Routing protocol for IEEE 802.11 infrastructure based wireless mesh networks,” J. Netw. Syst. Manage., vol. 18,no. 2,pp. 190-209, 2010.

[21] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMN's," IEEE Trans. Wireless Commun.,vol. 9, no. 5, pp. 1661-1675.

[22] V. V. V and V.M. A. Rajan, "Detection of colluding selective forwarding nodes in wireless mesh networks based on channel aware detection algorithm" MES J. Technol. Manage., pp. 62-66, 2011.

[23] Quiang Liu, Jianping Yin, Victor C. M.Leung, ZhipingCai, "FADE: Forwarding Assesment Based Detection of collaborative gray hole attacks in WMN's" IEEE Transactions on Wireless Communications, Vol. 12, no. 10, October 2013, pp. 5124-5137.

[24] J. Eriksson,M. Falaotsos, and S.V. Krishnamurthy, "Routing amid colluding Attackers," in Proc. 2007 ICNP, pp. 184-193

[25] Jaydip Sen " Security and Privacy issues in wireless mesh networks: A Survey" Wireless networks and security-Issues, Challenges and Research issues, Springer, pp. 189-272, Feb 2013.

[26] Sahil Seth, Anil Gankotiya, "Denial of service attacks and detection methods in wireless mesh networks" ITC 2010, pp. 238-240.

[27] Vikas Solomon Abel " Survey of attacks on mobile adhoc wireless networks" International journal on computer science and engineering (IJCSE) Vol. 3, No. 2, Feb 2011.

[28] Y. Sun, W. Yu, Z. Hun, and K. J. R. Liu, "Trust modelling and evaluation in ad hoc networks," in Proc. IEEE GLOBECOM '05, vol. 3, Dec. 2005.

[29] F. Oliviero and S. P. Romano, "A reputation-based metric for secure routing in wireless mesh networks," in Proc. 2008, GLOBECOM, pp. 1-5.

[30] Gao Xiaopeng and 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, Sept 2007.

[31] J. Sen, M. Chandra, S.G. Harihara, H. Reddy and P.Balamuralidhar, "A Mechanism for Detection of Gray Hole Attacks in Mobile Ad Hoc Networks", Proc. IEEE International Conference on Information Communication and Signal Processing ICICS, Singapore, Dec. 2007.

[32] J. B. Othman, J. P. Claude, Y. I. S. Benitez, "A Novel Mechanism to Secure Internal Attacks", IEEE ICC 2012-Ad-hoc Sensor Networking Symposium.

[33] Piyush Agrawal, R.K. ghosh, Sajal K. Das, "Cooperative Black and Gray Hole attacks in Mobile Ad Hoc Networks", In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.

[34] R. Kandikattu, L. Jacob, : A Secure intra-domain routing protocol for wireless mesh networks, Springer LNCS 4812, pp. 37-50 (2007).