Indian Journal of Science and Technology, Vol 9(41), DOI: 10.17485/ijst/2016/v9i41/86053, November 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Survey of Single and Cross Layer Security in MANET

G. Usha[1*], S. Kannimuthu[2], Karthik[3] and Gayathri Devi[4]

[1]Department of Software Engineering, SRM University, Kattankulathur, Kanchipuram – 603203, Tamil Nadu, India; ushag2@gmail.com
[2]Department of CSE, Karpagam College of Engineering, Coimbatore - 641032, Tamil Nadu, India; kannimuthu.me@gmail.com
[3]Department of IT, Karpagam College of Engineering, Coimbatore – 641032, Tamil Nadu, India
[4]Department of IT, Coimbatore Institute of Engineering and Technology, Coimbatore – 641109, Tamil Nadu, India.

Abstract

Various types of portable devices and military applications uses MANET. MANET is infrastructureless one and the security of such a network is a big issue. The detection of misbehavior and intrusions should be done before the attackers affect the network communication so as to keep MANET secure. In this article, a survey regarding single layer and cross layer security solutions for MANET is presented. This paper analyzes the techniques involved in detecting the attacks in each scheme. In this paper the security solutions using single (network) layer against black hole attack is discussed first. Secondly, a brief discussion of cross layer security of the existing works against security attacks using cross layer are given. Finally, the survey is concluded by highlighting open research issues in the field.

Keywords: AODV, Cross Layer Security, MANET, Packet Delivery Ratio, Single Layer Security

1. Introduction

Infrastructure less nature of MANET is useful to a variety of fields of science and technology: To gather information in commercial region, collaborative work, local, personal area and various types of applications MANET's are used[1].

On the other hand, security in MANET is an important issue[2]. The features of MANETs such as infrastructure less, multi-hop, autonomic node movement, amorphous nature, power limitation, memory and computation power limitations put up more at risk to attacks than customary networks. Security attacks against MANET are of four categories: External, Internal, Passive and Active. External attacks are caused by other nodes outside the network. Internal attacks are caused by the internal nodes in the network. Passive attacks are caused by continuous collection of information that can be launched as an active attack later. Active attacks are actively interacting with victims like sleep deprivation attacks, hijackstricting, jamming, and denial of service attack. Nowadays instead of providing single layer security, cross layer security solutions are proposed by various authors[3–5].

Cross layer security is known as exchange of information among the layers. The nodes in MANET move here and there. Providing single layer security is not enough[6,7] in MANET because of dynamic nature. Hence providing cross layer security is the alternative approach to secure MANET form various attacks. The organization of the paper is as follows. Section 2 portrays the problems and challenges of MANET security. Section 3 presents the vulnerabilities of black hole attack in MANET. Section 4 presents single layer security solutions in MANET. Section 5 presents the taxonomy of cross layer security solution in MANET. Finally we conclude and discuss the future research trend in Section 6.

2. Problems and Challenges of

*Author for correspondence

MANET Security

A MANET consists of dynamic, self-configuring, self-deployable nodes, where each node acts as a router. Unlike cellular or wired networks, MANETs do not require any base station or centralized routers; due to their Ad hoc nature[8,9]. MANET has variety of applications include military, disaster management, sensor networks, enhanced cellular networks, and delay-tolerant networks. The nodes in the network for MANET join and leave the network at any time. The links are getting disconnected at any time for MANET routing protocols have different routing strategies to forward packets.

Routing protocol in MANET is not designed to secure against malicious attackers. Various routing algorithms are proposed to handle attackers[10,11]. Routing protocols in MANETs are broadly categorized into two types: reactive routing protocols, and proactive routing protocols[12]. Reactive routing protocols are also known as on-demand routing protocols. In other words, table-driven routing protocols periodically exchange topology information. MANET routing protocols undergo from various kinds of attacks. Initially, the protocol designers assumed that the MANET environment is trusted, cooperative and did not consider about security. As a result, the malicious attackers disrupt the route and violate the protocol rules and drop the packets. The strict architecture of layered network in MANET is not sufficient to deal with the dynamics of a wireless network environment. Especially, the security of MANETs cannot be solved in isolation in a single layer. Cross layer methodology is used to enhance the network performance by exchanging or sharing the information between the layers. Various cross layer techniques are used to provide security in MANET[13]. Figure 1 explains the taxonomy of attacks.

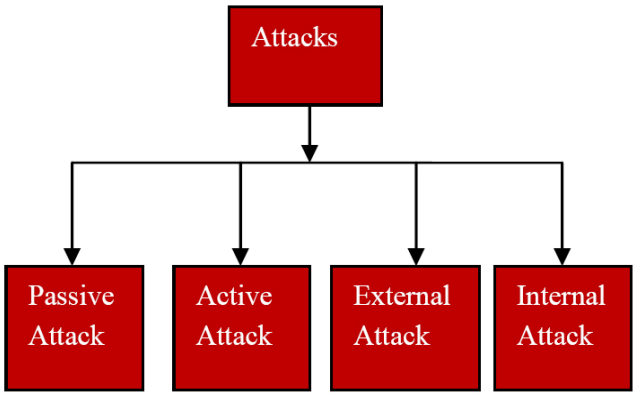

Figure 1. Taxonomy of attacks.

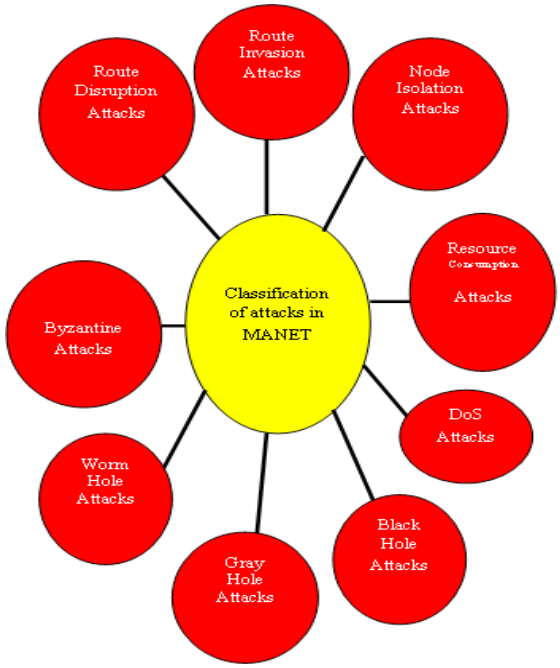

Figure 2. Classifications of attacks in MANET.

Passive attack won't change any network information. But it overhears or tries to get valuable information on the network.

Active attack interrupts the network by involving modification, interruption, and fabrication.

External attacks are not part of the network. They are carried out from outside the network domain.

Internal attacks are part of the network, and carried out from compromised hosts. Attacks in MANET are broadly classified as shown in Figure 2.

Route Disruption Attacks: Route disruption attacks mistreat or break the legitimate data packets in a dysfunctional way.

Route Invasion Attacks: Route invasion attack introduce a node between a source and the receiver.

Node Isolation Attack: Node Isolation attack separates a node from communicating with the other nodes in the network[13].

Resource Consumption Attack: Resource consumption attack consumes battery resources, and communication network bandwidth[14,15].

Denial of Service (Dos) Attack: Dos attack diminishes or eliminates the network capacity. These attacks are mainly

focused on attacking the server resources and network bandwidth[16].

Black Hole Attack: Black hole attack drops the packets between sender and receiver nodes[17,18].

Gray Hole Attack: This attack drops the packets maliciously for some time duration by dropping packets, and behave normally other times[19].

Worm Hole Attack: Worm hole attack where the attacker records a packet in particular locations and creates a tunnel in order to forward the packet to another location[20].

Byzantine Attack: Byzantine attack is where the malicious behavior of nodes cannot be detected because more than one node collude and cooperate with the others in such a way that the malicious behavior cannot be detected[21].

Rushing Attack: Rushing attack where the colluding attackers join together to transmit packets, which form a worm hole and make the transmission faster than other legitimate nodes[22]. Hence securing MANET is the challenging issue and important research area.

3. Vulnerabilities of Black Hole attacks in MANET

MANET layers got affected by various types of attacks[23]. The most vulnerable attacks in MANET are Black Hole attack and Gray Hole attack because these two attacks are type of active attack[24]. These active attacks can happen at any time in the network since these active attacks modify the normal operation of MANET and detecting these attacks is very hard[25].

Black Hole attack is a one kind of DoS attack and it is a severe threat against routing protocol which is done by dropping the packets. DoS attacks are effortlessly employed against routing in MANET. The major intention of this attack is to make the receiving node unreachable or downgrade the communication throughout the network. The unseen act of Black Hole nodes can be noticed by only observing the lost traffic. Black Hole attack drops all the packets in the communication path. Now we describe about the black hole attack with the help of AODV protocol. AODV handles two types of operation path discovery and path maintenance[26]. In MANET, when a sender node indend to communicate with other node, the sender node broadcasts a Route Request (RREQ) packet for the particular destination. The intermediate nodes broadcast the packets to the destination node. For example in the following Figure 3 the source node S wants to communicate with the destination node D. Initially, the source node S forwards the RREQ packets in the network. The nodes in the communication range checks its own routing table and also checks whether it is the destination node or it has a route to the destination node. If the specific node is not the destination node the nodes forward the packets. In below, in Figure 3 node A is not destination node, so node A again broadcasts the packets in the network. Now we explain how black hole attack occurs using AODV RREP packet. Now assume Node A is the malicious black hole node. Node A in Figure 3 which is a malicious node can forge a RREP message to the source node S. When source node S receives faked RREP message from node A, it updates its route to the destination node through a (non-existent) node.

Node A forwards the data packets. The RREP messages are copied by node A in following technique

- Making the hop count value is equal to one.

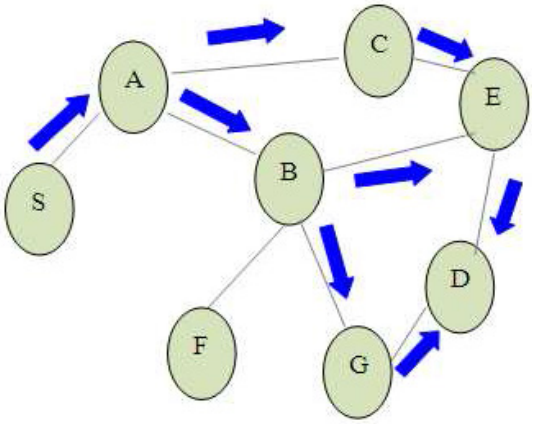

Figure 3. AODV route discovery using RREP packet.

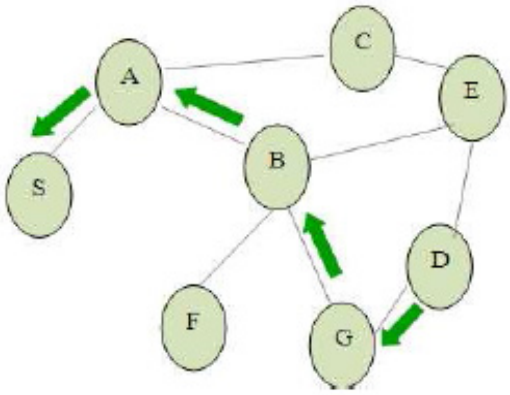

Figure 4. AODV route discovery using RREP packet.

- Destination sequence number is increased by at least one.
- Nonexistence IP address is assigned to the hop count address.
- The faked RREP messages are unicasted through out the network and the black hole node forwards the malicious packets.

Node S updated that the node D is the next node in its routing table. The malicious node D become the part of the network. Thus node A becomes the part of MANET and does all vulnerable behavior. Thus node A does all malicious behavior inside the network.

Thus node D forwards all the messages through node A. Thus the malicious node A becomes part of the network.

4. Single Layer Security Solutions against Black Hole Attack

MANET endures from various kinds of attacks in network layer that they suffer for various types of[27,28]. Many solutions have been proposed in literature to overcome these attacks.

4.1 Solution 1: Modification in AODV Routing Table

A new protocol is proposed by[29] in which they modified the existing AODV protocol, by adding a table known as Data Routing Information table (DRI), and also added a cross checking method. This DRI table consists of two entries, known as "From" and "Through", where from consists of the routing information where the packet starts and forwards the packets. In their model, every node maintains the extra information in the DRI table where "1" represents true and "0" represents false. At first, the source node sends the RREQ message to each node, the intermediate nodes send this request to the Next Hop Nodes (NHN), along with it's the DRI table. The source node cross checks this intermediate node's information with its own information. Thus, the source node inquires the intermediate nodes about its own DRI table and NHN information. In this way the source node estimates the honesty of the intermediate nodes. Mohammad.

A timer[30] based security solution is used in the existing AODV protocol by setting a timer, which stores the information such as request from other nodes and the information on the first request. This technique stores the packet's DSN information and received time in the Collect Route Reply Table (CRRT). From this table, the timeout count of the RREQ is calculated and judged whether the route is valid or not, based on the threshold value. Another technique [31] detects and prevents t Black Hole attacks in MANET using following manner. In their model, the initial process is the total count of messages which is to be sent from source to destination and calculated. Next, the message is broadcasted to the destination node. Simultaneously, a timer is set to check the time of which the destination receives the data packets. If the received data packets by the destination node are less than the predefined value, the removal of the Black Hole attack is initialized.

A new control packet known as ALARM[32,33] is introduced in AODV protocol. The RREP DSN is checked in order to know that it is greater than the value of threshold. If the value of RREP DSN is higher than the threshold value, then that sender is treated as the attacker and this information is updated in black list. Additionally, the threshold is calculated based on the average of the destination DSNs between the DSN and RREP packet in each time slot. This technique not only detects Black Hole attacks but also prevents the attack by updating the threshold value based on the network dynamics. A secured AODV[34] protocol is proposed known as Secure AODV (SAODV) to secure the AODV protocol. The main difference between the AODV and their proposed SAODV is in the route discovery process. The SAODV verifies the routes by exchanging a random number. However the normal AODV uses the DSN to verify the routes.

Another technique[35] is proposed which consists of two parts to detect and responds Black Hole attacks. In RREP packet, the next hop field is added additionally. The RREP packet has the examined by source nodes before sending the data packets. Next a new table[36] is added which is called as Cmg_RREP_Tab, a timer known as MOS_WAIT_TIME. Initially the source node sends the first RREP packet until it receives the RREP control message. The other variable mali_node stores the malicious node id. In this technique, initially the additional function Pre_Receive Reply is executed. The RREP packets stored in Cmg_RREP_Tab are analyzed by the source node. Then, the RREP packet which has the highest DSN is compared to the source node which is suspected as malicious node. Finally, the packets from the suspicious node are discarded, i.e., the control messages coming from suspicious node is ignored.

An Anti-Black Hole Mechanism[37] (ABM) is proposed in which an intrusion detection technique is proposed, where all nodes maintain this ABM. If an intermediate node has not broadcast any RREQ message, it is marked as suspicious node. Additionally, another new table which is known as the new block table is added to the original table to record the details of Black Hole nodes. The initial detection process begins by executing the ABM function in a sniff mode. Based on the threshold value, if the routing information difference exceeds, it is marked as a Black Hole node. If the normal node receives the RREP message from the Black Hole node, it drops the RREP packet. A trust table[38] is added in AODV protocol. A new trust table and a timer is used to compute the amount of time a node is waiting to receive the route reply from other nodes. Based on the trust value a node is identified as malicious node.

4.2 Solution 2: Neighborhood based Detection

A neighborhood based detection[39] technique is proposed to detect the Black Hole attacks. The authors used a route recovery protocol to establish a path to the correct destination node. Their detection technique involves three main steps: First the source node collects the neighbor set information. The second step determines the Black Hole nodes by computing the threshold value and the third step involves the use of the cryptography based authentication technique to identify the true destination node.

4.3 Solution 3: Cooperative Detection Technique

In order to find cooperative attack, distributed and co-operative mechanism[40] is proposed. Many techniques are used to detect various types of attack and various tables are used to mark the network information.

A cooperative solution is discussed[41] to prevent cooperative Black Hole attacks in MANET. In their work they used few additional fields in AODV to detect the Black Hole attacks. The DRI table is used for checking the Further Request (FREQ) and Further Reply (FREP) packets. By using these messages Black Hole attacks are detected. Their technique trusts the destination node as genuine node. During the time of each route establishment, the source node checks the intermediate nodes to ensure that the source node has already established a connection with the intermediate nodes previously. If the connection is already established between the source and intermediate nodes, then the transmission is carried out through the established path. This scheme has many drawbacks. For example, if a new node joins as an intermediate node, then their method considers the new node as a malicious node.

A secure routing[42] technique which is based on honesty about the reply of the node is discussed. In order to participate in the routing process, a node has to prove its honesty. If a node is the first receiver of a RREP packet, it forwards packets to source and initiates the judgment process on replier. The judging process is based on the opinion of network's nodes about replies. The activities of a node are logged by its neighbors. These neighbors are requested to send their opinion about a node. When a node collects all opinions of the neighbors, it decides that the replier is a malicious node. The decision is based on a number of rules. In the first rule, if a node delivers many data packets to destinations, and the sender node is assumed as an honest node. In the second rule, a node receives many packets but do not send same data packets, it is possible that the current node is a malicious node. In the third rule, the current node has to send a number of RREP packets. By using these rules, the Black Hole node is detected from the network.

A new detection[43] scheme known as react scheme was proposed. When the communication between a source node and destination node drops lower, the react scheme is automatically triggered. This react scheme consists of three phases: namely audit phase, search phase and identification phase. In their technique, a target node sends a feedback to the sender node when the PDR is larger in the network. Then, a bloom filter is used to know the behavior proof of the nodes in the network. Finally, the malicious node's segment location proof is compared with source node's behavioral proof to make a final decision.

4.4 Solution 4: Bayesian Detection Technique

A Bayesian technique[44] is proposed to detect against Black Hole attack in MANET. For monitoring the attack, a random two-hop acknowledgement technique is employed. A local judgment method based on bayesian analysis is used in their model to detect attacks in the detection phase. When a node is marked as malicious node, judgment must be approved by all the other nodes in the network. In order to apply these judgments, additionally they used a witness-based protocol.

4.5 Solution 5: Analytical based Detection Technique

An analytical framework is[45] proposed to analyze various types of DoS attacks in MANETs. They focused mainly on jellyfish and Black Hole attacks. Zhao Min & Zhou Jiliu (2009) proposed a hash based authentication mechanism for enhanced security. Techniques used in their works are used to offer quick message verification and group identification which discovers the collaborative suspicious nodes and identifies the secure routing path in order to prevent Black Hole attacks. In order to use public key infrastructure in MANET, each node maintains a secret key. The source node checks for secret key whenever it receives packets from the neighbors. The sharing secret key is undisclosed to the participants among the network. After checking the above conditions, the packet is confirmed as available packet and the routing is confirmed as secure routing.

4.6 Solution 6: Data Mining based Detection Technique

Anomaly based detection technique is proposed[46] in MANET. In this technique, the Principal Component Analysis (PCA) technique is used to detect black hole attack. Their technique consists of learning phase and monitoring phase. In the learning phase, the system collects the packets from network traffic. In the monitoring phase, the features are collected within a particular time limit. Using PCA, the recorded features are represented as a p dimension vector. In learning phase, the first principal component is calculated in order to identify the normal profile. The PCA is applied to the collected data of the first monitored time slot. The deviation is observed from the first principal component. If the deviation exceeds, the calculated threshold value, the IDS presumes that an attack takes place. Otherwise, the data from the next monitored time turns into the new profile.

4.7 Solution7: Authentication based Detection Technique

A client server model[47] is proposed to detect black hole attack in MANET. Whenever a node (client) request came to join the network, the server receives the request packet from the joining node. The server node generates a membership acknowledgement packet for the client node. If the client node does not reply within a certain amount of time then the server discards the joining request of the client node. On the other hand, if the client node accepts for membership acknowledgement, its details are added into the database and the new client node is assigned Node Code (NC), packet key 1 and packet key 2. After becoming the member of the network, the node sends the request for the shortest path with the key packet key 2. If the key packet key 2 matches with packet key 1 then the server establishes a connection between the client and server. This technique uses the server as a central authority for communication.

5. Cross Layer Security Solutions against Black Hole Attack

5.1 Solution 1: Cross Layer Data Collection Security

A cross layer based[48] interaction among the layer is proposed which is used to understand about the layer interactions. They proposed that cross layer interaction can be done between the routing layer and the physical layer, the routing layer and the MAC layer, the TCP layer and the application layer. These modifications are done in order to improve the network performance such as Quality of Service (QoS), security and so on.

A different kind of layer interaction[49] is presented with various types of interactions between the layers. The information flows between the layers, they can be like upward information flow, downward information flow, back-and-forth information flow, merging of adjacent layers, design coupling without new interfaces and vertical calibration. Upward information flow depicts the information that is transferred from lower layers to upper layers. Downward information flow indicates the information flow from upper layers to lower layers. Back and forth indicates that the flow is iterative between two layers. Merging of layer denotes combining two layers.

5.2 Solution 2: Cross Layer Data Mining and Game Theory based Security

A cross layer based[50] defensive technique is proposed to defend against different type of black hole attacks in MANET. They used the architecture known as CARDS which uses machine learning algorithm to defend against security problems in MANET. Their technique consists of three modules namely data collection module, data reduction module and learning module. They

used the apriori algorithm to correlate the data. In the data reduction technique, they used support vector machines and Fischer discriminant analysis to classify the data.

A shared[51] data base model using cross layer design technique is proposed, which uses a shared database model. They proposed two types of architecture which are named as Type-I Cross layer IDS (CIDS) and Type-II CIDS architecture. In their technique, they proposed shared database model. The shared database model collects data's from physical, MAC and network layer. They detected misbehavior detection in Ad hoc networks. CIDS framework interacts with the Intrusion detection module using a cross layer management plane. The cross layer management plane is responsible for gathering specific parameter from different protocol layers. The IDS uses the cross layer information to identify and detect security threats and network misbehaviors.

6. Conclusion

In this paper we have survey about single layer security and cross layer security in MANET. Securing MANET against Black hole attack especially Denial of Service attack is still a research issue. Many researches proposed various solutions to defend against black hole attack using single layer and cross layer technique. But most of the security solutions are based on assumptions which they did not consider about real issue. Further the researchers can provide dynamic and realistic solutions to defend against these attacks.

7. References

1. Ali Dorri, Kheyrkhah SRKE. Security challenges in mobile adhoc networks: A survey. IJCSES. 2015; 6(1):15–29.
2. Zanoon N, Albdour N, Hamatta HAS, Al-Tarawneh RM. Security challenges as a factor affecting the security of manet: Attacks and security solutions. IJNSA. 2015; 7(3):1–13.
3. Yi S, Kravets R. Composite key management for ad hoc networks. Proceedings of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services; 2004. p. 52–61.
4. Hu Y, Johnson PA. A survey of secure wireless ad hoc routing. IEEE J of Security and Privacy. 2004; 2(3):28–39.
5. Yang H, Luo H, Ye F, Lu S, Zhang L. Security in MANETs: Challenges and solutions. IEEE J of Wireless Communications. 2003; 11(1):38–47.
6. Agrawal P, Ghosh RK, Das SK. Cooperative black and gray hole attacks in MANETs. Proceedings of ACM 2nd International Conference on Ubiquitous Information Management and Communication; 2008. p. 310–4.
7. Bounpadith K, Nakayama H, Nemoto Y, Kato N, Jamalipour A. A survey of routing attacks in MANETs. IEEE Transactions on Wireless Communications. 2007; 14(5):85–91.
8. Lima M, Dos Santos AL, Pujolle G. A survey of survivability in MANETs. IEEE Communications and Surveys. 2009; 11(1):66–77.
9. Bose U. Comparing the impact of black hole and gray hole attacks in mobile adhoc networks. Procedia Computer Science. 2012; 8(11):1788–802.
10. Agrawal P, Ghosh RK, Das SK. Cooperative black and gray hole attacks in MANETs. Proceedings of ACM 2nd International Conference on Ubiquitous Information Management and Communication; 2008. p. 310–4.
11. Nasipuri A, Casaneda R, Das SR. On-demand multipath routing for MANETs. Proceedings of IEEE INFOCOM; 1999. p. 64–70.
12. Bounpadith K, Nakayama H, Nemoto Y, Kato N, Jamalipour A. A survey of routing attacks in MANETs. IEEE Transactions on Wireless Communications. 2007; 14(5):85–91.
13. QiWang MA, Abu-Rgheff. Cross layer signalling for next generation wireless systems. Proceedings of Wireless Communications and Networking; 2003. p. 1084–9.
14. Vidhya UK, Priya AM. A novel technique for defending routing attacks in OLSR MANET. Proceedings of IEEE International Conference on Computational Intelligence and Computing Research; 2010. p. 1–5.
15. Jawandhiya PM, Ghonge MM, Ali MS, Deshpande JS. A survey of MANET stacks. International Journal of Engineering Science and Technology. 2010; 2(9):4063–71.
16. Denko MK. Detection and prevention of Denial of Service (DoS) attacks in MANETs using reputation-based incentive scheme of systemic. Cybernetics and Informatics. 2006; 3(4):1–9.
17. Ning P, Sun K. How to misuse AODV: A case study of insider attacks against mobile ad hoc routing protocols. Proceedings of the 4th Annual IEEE Information Assurance Workshop; 2003. p. 60–7.
18. Subathra P, Sivagurunathan S, Ramaraj N. Detection and prevention of single and cooperative black hole attacks in MANETs. International Journal of Business Data Communications and networking. 2010; 6(1):38–57.
19. Xiaopeng G, Wei C. A novel gray hole attack detection scheme for MANETs. Proceedings of IEEE IFIP International Conference on Network and Parallel Computing Workshops; 2007. p. 209–14.

20. Ilyas M. The handbook of ad hoc wireless networks. CRC Press; 2003.
21. Awerbuch B, Holmer D, Nita-Rotaru C, Rubens H. An on-demand secure routing protocol resilient to byzantine failures. Proceedings of the ACM Workshop on Wireless Security; 2002. p. 21–30.
22. Yang H, Luo H, Ye F, Lu S, Zhang L. Security in MANETs: Challenges and solutions. IEEE J of Wireless Communications. 2003; 11(1):38–47.
23. Shen XX, Du DZ. A survey on attacks and countermeasures in MANETs. Proceedings of Wireless/Mobile Network Security Signals and Communication Technology; 2006. p. 103–35.
24. Taggu A. Trace gray: An application-layer scheme for intrusion detection in MANET using mobile agents. Proceedings of 3rd International Conference on Communication Systems and Networks; 2011. p. 1–4.
25. Zapata M. Secure Ad hoc On-Demand Distance Vector (SAODV); 2002. Available from: www.cs.ucsb.edu/~ebelding/txt/saodv.txt
26. Fantahun Y, Zhao A, Xuan C. Preventing black hole attack in mobile ad-hoc networks using anomaly detection. Proceedings of 2nd International Conference on Future Computer and Communication (ICFCC); 2010. p. 21–4.
27. Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures of ad hoc networks. 2003; 1(3):293–315.
28. Zhang W, Rao R, Cao G, Kesidis G. Secure routing in ad hoc networks and a related intrusion detection problem. Proceedings of IEEE Conference on Military Communications; 2003. p. 735–40.
29. Chun H, Johnson D, Perrig A. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Journal of Ad hoc Networks. 2003; 1(1):175–92.
30. Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K. Prevention of cooperative black hole attack in wireless ad hoc networks. Proceedings of International Conference on Wireless Networks; 2003. p. 23–6.
31. Tamilselvan L, Sankaranarayanan V. Prevention of black hole attack in MANET. Proceedings of IEEE 2nd International Conference on Wireless Broadband and Ultra Wideband Communications; 2007. p. 27–30.
32. Banerjee S. Detection/removal of cooperative black and gray hole attack in MANETs. Proceedings of the World Congress on Engineering and Computer Science; 2008. p. 85–97.
33. Raj PN, Swadas PB. DPRAODV: A dynamic learning system against black hole attack in AODV based MANET. International Journal of Computer Science. 2009; 54–9.
34. Lu S, Li L, Lam K-Y, Jia L. SAODV: A MANET routing protocol that can withstand black hole attack. Proceedings of International Conference on Intelligence and Security; 2009. p. 421–5.
35. Jaisankar N, Saravanan R, Swamy K. A novel security approach for detecting black hole attack in MANET. Proceedings of Springer International Conference on Recent Trends in Business Administration and Information; 2010. p. 217–23.
36. Mistry N, Jinwala DC, Zaveri M. Improving AODV protocol against black hole attacks. Proceedings of International Multi Conference of Engineers and Computer Scientists; 2010. p. 17–9.
37. Su MY. Prevention of selective black hole attacks on MANETs through intrusion detection systems. J of Computer communication. 2011; 34(1):107–17.
38. Mahmood AA, Hasan TM, Ibrahim DS. Modified AODV routing protocol to detect the black hole attack in MANET. International Journal of Advanced Research in Computer Science and Software Engineering. 2015; 5(7):173–8.
39. Sun B, Guan Y, Chen J, Pooch UW. Detecting black-hole attack in MANETs. Proceedings of 5th European Personal Mobile Communications Conference; 2003. p. 22–5.
40. Wu C, Wu TK, Cheng RH, Chang SC. A distributed and cooperative black hole node detection and elimination mechanism for ad hoc network. Lecture Notes in Computer Science. 2007; 4819:538–49.
41. Weerasinghe H, Fu H. Preventing cooperative black hole attacks in MANETs: Simulation implementation and evaluation. Proceedings of IEEE Future Generation Communication and Networking; 2007. p. 362–7.
42. Medadian MMH, Yektaie A, Rahmani M. Combat with black hole attack in AODV routing protocol in MANET. Proceedings of IEEE International Conference on 1st Asian Himalayas. 2009. p. 1–5.
43. Kozma W, Lazos L. REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits. Proceedings of 2nd ACM Conference on Wireless Network Security; 2009. p. 103–10.
44. Djenouri D, Badache N. Struggling against selfishness and black hole attacks in MANETs. Wiley Wireless Communication and Mobile Computing. 2008; 8(6):689–704.
45. Aad I, Hubaux JP, Knightly EW. Impact of denial of service attacks on ad hoc networks. IEEE/ACM Transaction on Networking. 2008; 16(4):791–802.
46. Nakayama H, Kurosawa S, Jamalipour S, Nemoto Y, Kato N. A dynamic anomaly detection scheme for AODV based MANETs. IEEE Transactions on Vehicular Technology. 2009; 58(5):2471–81.
47. Bajwa SS, Khan MK. Grouped Black Hole Attacks Security Model (GBHASM) for wireless ad-hoc networks.

Proceedings of 2nd International Conference on Computer and Automation Engineering; 2010. p. 756–60.
48. Min Y, Yao T, Quan Y. Cross layer ideas in wireless network designs. Proceedings of IEEE International Symposium on Wireless Communications; 2005. p. 891–4.
49. Srivastava V, Motani M. Cross layer design: A survey and the road ahead. IEEE Journals and Communication magazine. 2005; 43(12):112–9.
50. Joseph JFC, Lee B-S, Das A, Seet B-C. Cross layer detection of sinking behavior in wireless ad hoc networks using SVM and FDA. IEEE Transactions on Dependable and Secure Computing. 2011; 8(2):233–45.
51. Thamilarasu G, Sridhar R. CIDS: Cross layer intrusion detection system for MANETs. Proceedings of IEEE International Journal of Mobile Ad hoc and Sensor Systems Conference; 2009. p. 855–61.