ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Isolation of Black Hole Attack with Intrusion Detection System – A Survey

[1]T.Manikandan, [2]N.Kamaraj and [3]S.Dhivya

[1]*Department of Computer Science and Engineering,Thiagarajar College of Engineering, Madurai-625015, India.*
[2]*Department of Electrical and Electronics Engineering,Thiagarajar College of Engineering, Madurai-625015, India.*
[3]*Department of Computer Science and Engineering,Thiagarajar College of Engineering, Madurai-625015, India.*

ARTICLE INFO

Article history:
Received 12 March 2015
Accepted 28 April 2015
Available online 5 May 2015

Keywords:
MANET, Black hole Attack, Intrusion Detection System.

ABSTRACT

MANET is an infrastructure less system of portable nodes. Security issues in MANET are a testing assignment these days. Because of its dynamic nature MANET are at more vulnerable to attacks. IDS can be defined as the method, which helps to identify and report any unauthorized or unapproved activities in network or system. Black hole attack occurs in network layer which degrades the reliability of the message transfer by dropping the packets. This paper deals with black hole attack against Optimized Link State Routing (OLSR) convention with Intrusion detection system. We examine in detail the effect of this attack with a specific end goal to demonstrate the need for a countermeasure to attack.

To Cite This Article: T.Manikandan, N.Kamaraj and S.Dhivya., Isolation of Black Hole Attack with Intrusion Detection System – A Survey. ***Aust. J. Basic & Appl. Sci.,*** *9(7): 750-755, 2015*

INTRODUCTION

MANET is a self-configurable mobile system, which is infrastructure less with no central administration. MANET is suitable to various applications such as military, disaster recovery, personal area network and more. Each node communicates with the other acting as routers. MANET are susceptible and defenseless to malicious attack because of its features like open medium, lack of central administration, dynamic topology changes, cooperative algorithms and so on. Snooping attacks, black hole attacks, wormhole attacks, routing table overflow, packet replication, distributed DoS (DDoS) attacks, denial of service attacks (DoS), etc are various kinds of attacks to which MANET is exposed.

In this paper we define black hole attacks in OLSR routing protocol in mobile Ad-Hoc network. Therefore, the improvement of steering conventions in MANET is amazingly difficult. Some of the security issues present in MANET are dynamic in nature so prior trust relationship between the nodes cannot be derived. MANET consists of hundreds or even thousands of nodes so security mechanisms should be scalable to handle such a large network. Limited energy supply and mobility of the nodes makes the wireless link unreliable which is not consistent for the nodes involved in communication. Because of the movement of the nodes the routing information is changed continuously which leads to lack of incorporation of security features (Wu B, Chen J *et al* 2011). Now let's discuss about the black hole attack that occurs in MANET and the contribution of IDS on improving the efficiency of the network.

2. Related Work:

IDS can be defined as the method, which helps to identify and report any unauthorized or unapproved activities in network or system. It collects and analyses the activity information to determine any unusual activity. If any misbehavior occurs it will generate an alarm to alert the security administrator. The types of IDS are stand alone IDS in which IDS run on each node independently but cooperation between the nodes does not exist. The second one, Distributive and cooperative IDS is more suitable for flat network infrastructure but not suitable for multilayer .Here every node has an individual IDS agent running on them which is responsible for detecting and collecting local data (H. Debar *et al*., 1998). It is useful to identify possible intrusion; each node participates in intrusion detection system. The third one, hierarchical IDS have been proposed for multilayered network infrastructure. In hierarchical IDS the network is divided into cluster which in turn each cluster has cluster heads (M. Asaka *et al*., 2007). The cluster heads sometimes act as control points similar to

Corresponding Author: T. Manikandan, Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, India.
E-mail: tmcse@tce.edu

routers, switches, gateway in wired network. They have more responsibility and functionality when compared to other members in cluster. The various kinds of detection are

Anomaly detection:

In an anomaly detection system a baseline profile of normal system activity is created. Any system activity that deviates from the baseline is treated as a possible intrusion. One advantage in this technique is that they do not look for something specific and also eliminates the known attack vectors and keep this attack dictionary current (Robert mitchell,Ing-ray chen2014). The problems with strict anomaly detection are that:

• Anomalous activities that are not intrusive are flagged as intrusive.

• Intrusive activities that are not anomalous result in false negatives.

One disadvantage of anomaly detection for mobile computing is that the normal profile must be periodically updated and the deviations from the normal profile computed. The periodic calculations can impose a heavy load on some resource constrained mobile devices; perhaps a lightweight approach that involves comparatively less computation might be better suited.

Misuse detection:

In misuse detection, decisions are made on the basis of knowledge of a model of the intrusive process and what traces it ought to leave in the observed system.

Legal or illegal behaviour can be defined and observed behaviour compared accordingly. Such a system tries to detect evidence of intrusive activity irrespective of any knowledge regarding the background traffic (i.e., the normal behaviour of the system).

Specification-based detection:

Specification based detection defines a set of constraints that describe the correct operation of a program or protocol, and monitors the execution of the program with respect to the defined constraints. This technique may provide the capability to detect previously unknown attacks, while exhibiting a low false positive rate.It looks for unusual performance at the system level and (Robert mitchell,Ing-ray chen2014). One major advantage of specification based intrusion detection is a low false negative rate

Signature-based detection:

A signature based IDS will comparing the packets on the network and also monitor those packets on the network from the known malicious activities and it looks for runtime features that match a particular pattern of misbehavior (Robert mitchell,Ing-ray chen2014).

A. Watchdog:

The Watchdog scheme consists of two parts namely watchdog and pathrater. Watchdog method detects misbehaving nodes that aims to improve throughput of network (Anuj Gupta *et al* 2011). The watchdog identifies the misbehaving nodes by eavesdropping on the transmission of the next hop. If a node does not send a packet in a specified time it is marked as susceptible node. If the node behaves susceptible several times determined by a Threshold value, it is marked as misbehaving node. The advantages of watchdog are it is very simple and easy to implement and the power consumption is very less.

Next one is path rater which combines knowledge of misbehaving nodes and routing protocols to avoid the reported nodes in future transmission. Every node is maintaining a rating for each other node it knows about in the network and path metric is calculated by averaging the node ratings in the path. If multiple paths exist to the same destination, the path with the highest safety metric is chosen and also it detects the misbehaviours at the forwarding level (Serigo Marti,T.J.Giuli,Kevin lai and Mary baker 2000). The drawbacks of watchdog are receiver collision which takes place when two nodes are trying to sends packet at the same time to another node. In order to preserve its own battery resources some nodes purposely limited its transmission power .when a node purposely report other node as misbehaviour even if the node forward the packet to destination is known as false misbehaviour report. The attackers can easily capture and compromise one or more nodes to achieve this attack and also it might not detect the malicious are misbehaviour nodes (Serigo Marti,T.J.Giuli,Kevin lai and Mary baker 2000) in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehaviour, collusion and partial dropping.

B. Eaack:

EAACK is Hybrid scheme which mitigates weaknesses like false misbehaviour, limited transmission power, receiver collision. (M. Al-Shurman, S-M.*et al*, 2004), (S. Kurosawa *et al*.,2006) it is specially designed for MANET to detect the attackers. EAACK is acknowledgement based scheme which makes use of digital signature. This scheme requires acknowledgement for every packet sent from sender to receiver and all the acknowledgement packets must be digitally signed before sending and verified by the receiver.

3. Characteristics of Intrusion Detection System:

An IDS collects and analyses audit data to detect unauthorised uses and misuses of computer systems (Dorothy E. Denning,*et al* ,2011).

To present the characteristics of IDS we will use the following criteria, defined by the IBM labs in

(Zurich H. Debar, M. Dacier, and A. Wespi,*et al* 1998).

– Audit source location: The data to be analysed may be obtained on the host, in application or system log files by Host Based Intrusion Detection Systems (HIDS) or from the network (for instance, by placing sniffers on interconnection equipment) by Network Based Intrusion Detection System(NIDS).

– Methodology of detection: Two approaches are used for the detection of intrusions:

They are Anomaly detection and misuse detection. With anomaly detection, the system knows the user's standard profile and detects deviations from this reference. Misuse detection, on the other hand, relies on the signature of attacks. Even though, commercial products tend to prefer signature based detection, neither of the two techniques has really proven better than the other and research in this field still remains active.

– Computing location: Most IDS use a centralised architecture to gather and analyse audit data. Some of them use agent technology to realise a local pre-analysis prior to centralising the data.

– Usage frequency: An IDS can collect and analyse data at regular intervals or provide a continuous intrusion detection service. The latter is particularly needed by an open environment such as Internet where intrusions should be detected "on the fly".

– Response to intrusions: When an intrusion is detected the system may react in different ways. Most systems generate an alarm informing the administrator, who decides of the reaction to have. A more sophisticated response consists in a corrective action (a new rule in a firewall, disconnection of suspicious connections) to prevent an identical future attack.

4. Black hole Attack:

The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. The intruders utilize this loophole to carry out their malicious behaviours because the route discovery process is necessary and inevitable (C. Perkins *et al*., 2004). A black hole attack is referred to as a node dropping all packets which it is supposed to forward by claiming that it has the shortest path to the destination .The actual implementation of the black hole attack strongly depends on the deployed routing protocol.

a) Black Hole attack in OLSR:

In OLSR the system topology data is fabricated from HELLO and Topology control (TC) messages. A black hole node sends fake HELLO messages. In these messages the malicious node contend that it have a greater number of connections to neighbors than it really has. In this way, there is a bigger plausibility of selecting this node as a Multiple Point Relay (MPR) node of the source. The more neighbors the attacker node have, the bigger the conceivable impact of the attack. For example the node M is sending fake HELLO messages and there is always a possibility that it can act as Black hole node as show in Figure 1.

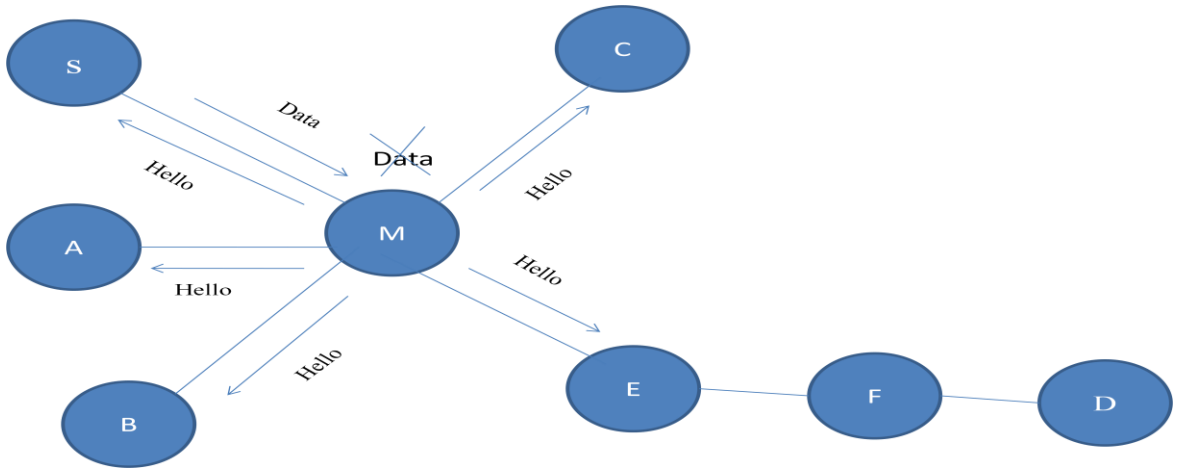

Fig. 1: Black hole attack in MANET

Table 1: Existing schemes for eliminating Black hole attack

Schemes	Routing Protocol	Simulator	Publication year	Results
Data routing information table scheme (Dixon and Kendall Nygard 2003)	AODV	NS-2	2003	Applicable to identify various black hole nodes in MANET and by avoiding multiple black hole node a secure path is created from source to destination.
Detection scheme based on	Secure AODV	GloMoSim	2007	The PDR of AODV is around 80% when

Time based (Da Zhang,Chai Kiat Yeo 2011)	(SAODV)			SAODV is around 90%to100% but when the malicious node is away from the source node the end-to-end delay increases
Bayesian Detection scheme and Random Two-hop ACK (Murty MS, Das MV 2011)	DSR	GloMoSim	2007	The true positive rate can achieve 100% when existing 2 witness but The proposed scheme is not efficient when k equals to 3reducing the true positives.
Guard node based scheme (Imran Raza,S.Ahussain 2008)	AODV	NS-2	2008	The process of identification of malicious node is dynamic and efficient based on the trust level of a node and also provides better throughput
Anti black hole mechanism (Ming-Yang Su2011)	AODV	NS-2	2010	The packet loss rate is reduced to about 10.05% (threshold set as 5) or 13.04% (threshold set as 10) and detection rate was 100%,
Path validation and attack finder message Ahmed (M.Abdalla,Imane 2011)	OLSR	NS-2	2011	By utilizing the backlist created, the misbehavior nodes are isolated from the network and broadcasting to other nodes in the network.
Based on the physical characteristics, authentication of the nodes and also overhead incurred in new route discovery process (M.Mohana priya,Ilango krishnamurthi,*et al* ,2014)	DSR	GloMoSim	2014	With the help of this scheme, the destination node will detects the presence of malicious node from the source route itself and also isolated from the network and also the promiscuous mode will be activated in case of some energy loss

b) Black hole attack mitigation with IDS:

The focal root cause for the black hole attack is that the routing protocol does not admit any confirmation for the Route established. Hence it is significant to procure a confirmation mechanism for the route established in the routing protocol. It is depleted by introducing a distinct mode of message called Route Confirmation Request (CREQ) and Route Confirmation Reply (CREP). These messages assist to keep away from black hole attack. Once the Destination node sends a RREP to source node furthermore it also sends a CREQ to its next bouncing node. If the next bounce node has a path to the source then it generates a CREP and forward it to the source node. Finally CREP reaches the source node following the RREP. . After accepting the CREP, the source node can affirm the authority of the way by contrasting the way in RREP and the one in CREP. In the event that both are matched, the source nodes judges that the course is right (S. Kurosawa *et al*.,2006). One downside of this methodology is that it can't keep away from the black hole attack in which two consecutive nodes work in agreement.

In (M. Al-Shurman, S-M. *et al* 2004) The black hole problem is one of the security attacks that occur in *mobile ad hoc networks* (MANETs). We present two possible solutions. The first is to find more than one route to the destination. The second is to exploit the packet sequence number included in any packet header. Computer simulation shows that compared to the original *ad hoc on-demand distance vector* (AODV) routing scheme, the second solution can verify 75% to 98% of the route to the destination depending on the pause times at a minimum cost of the delay in the networks.

The key advantage of this approach is that it can detect the attack at low cost without introducing extra routing traffic, and it does not require modification of the existing protocol. However, false positives are the main drawback of this approach due to the nature of anomaly detection (S. Kurosawa *et al*.,2006)

Taking into account this examination, the sender propose a measurable based aberrance recognition methodology to identify the black hole attack, in light of contrasts between the objective arrangement quantities of the received RREPs (Yang S-J, Lin Y-C *et al*., 2009). The key preference of this methodology is that it can distinguish the attack with ease without presenting additional steering activity, and it doesn't oblige adjustment of the current convention (Dow CR, Lin PJ *et al*., 2005). Nonetheless, false positives are the fundamental downside of this methodology because of the way of abnormality discovery (Zhou L, Chao H-C *et al*., 2006). In(F.T.seng,L.chou,C.chou ,2011) they surveyed existing solutions for detecting black hole Attack and classified these proposals either single or cooperative black hole attack. In (E.Padilla,N.Schenbruck,P.Maritini,m.Jhanke and J.Tolle 2007) there is an example for the detection using topology graph based on the no of neighbors claims to have and actual no of neighbors and this technique would not be effective in any other reactive protocols. Detecting black hole attack on AODV(M.Medadian,M.H.yektaie and A.M.Rehmani 2009) in which the neighbors shares their opinon about the replier and if the number of packets received which is not equal to certain number of sent packets is considered to be malicious. A detection scheme (X.Y.Zhang,Y.Sekiya andY.wakahara,*et al* 2009) which is based on sequence number of RREP packets and considered intermediate node is an attacker.

Table 2: Various existing IDS schemes for Black hole Attack

Schemes	Simulator	Publication year	Results
Local Intrusion detection system scheme(LIDS)(M. Asaka, A. Taguchi, and S. Goto,*et al*l,1999).		2004	This scheme was validated by implementation and the IDS messages and IDS rules are taken into three attacks and it is absolutely suited for MANET.
Conflict checking mechanism (Tseng Y-C *et al*., 2004)	Ns-2	2005	This scheme protects other types of proactive MANET routing protocols that are based on MPR Optimization and also shows that the approach effectively enhances the security level and fault detection capability of an OLSR MANET
Ex watchdog intrusion detection system (Nidal naseer *et al*., 2007)	Ns-2	2007	This scheme detects the falsely report other nodes as misbehaving and increases the network performance.
Detection in route establishment and data forwarding phase (Yuvaraj singh *et al*., 2011)	Ns-2	2011	In this scheme the detection effectiveness is more than 80%and also false positives are below 20%.
Distributed court system mechanism(Da Zhang,Chai Kiat Yeo,2011)	Ns-2	2011	It provides a way for accurate and timely detection of attacks and also increases IDs's in reducing false positive rate and suppressing malicious activities.
Improved IDS (IIDS) (Marti S *et al*., 2000)	Ns-2	2013	In the cases of receiver collision, the performances are optimistic against AACK and false misbehavior report and limited transmission power and also add more security to prevent attackers from data attacks
Hybrid key cryptography technique (Yang H, Lou H *et al* 2009) (Umang S *et al* 2011)	Ns-2	2014	EAACK schemes digital signature that causes network overhead which can be further reduced by hybrid key cryptography

Conclusion:

In this paper, we surveyed and analysed various Intrusion detection schemes in MANET to provide the designers a view to establish a system model with enhanced features of IDS. This would probably develop a MANET environment with high reliability. We also analyzed effects of black hole attacks and their influence in MANET. Our future work is to enhance the existing IDS mechanism that incorporate Trust based ids mechanism i.e. Trust based mechanism will be coupled with intrusion detection system that could ensure the security services required by users in MANET to improve the efficiency of the networks by detecting various attacks in MANET and isolating them thereby establishing a reliable network.

REFERENCES

Ahmed M. Abdalla, Imane A. Saroit, Amira Kotb, Ali H. Afsara, 2011. Misbehaviour nodes detection and isolation for MANETs OLSR Protocol.Procedia computer science 3(1Da Zhang,Chai Kiat Yeo,2011-1H. Debar, M. Dacier, and A. Wespi,*et al* 1998) in World conference on Information techonolgy.

M.Al-Shurman, S-M. Yoo, and S. Park, ―Black Hole Attack in Mobile Ad Hoc Networks, 2004. ACM Southeast Regional Conf.

Anuj Gupta, Navjot Kaur, Amandeep Kaur, 2011. "A Survey on Behaviour of AODV and OLSR Routing Protocol of Manets under Black Hole Attack" in IJCST, 2(4).

Asaka, M., A. Taguchi and S. Goto, 1998. The implementation of ida : An intrusion detection agent system. In proceeding of 11th FIRST Conference-Brisbane-Australia,1999.systems. IBM Zurich Research Laboratory, Ruschlikon, Switzerland.

Debar, H., M. Dacier and A. Wespi, 1998. A Approach on taxonomy of intrusion detection systems. IBM Zurich Research Laboratory, Ruschlikon, Switzerland.

Dow, C.R., P.J. Lin, S.C. Chen, J.H. Lin, S.F. Hwang, 2005. A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks. Paper presented at the IEEE 19th International Conference on Advanced Information Networking and Applications, Tamkang University, Taiwan, 28-M. Asaka, A. Taguchi, and S. Goto,*et al*l,1999 March 2005.

Imran Raza, S. Ahussain, 2008. Identification of malicious node in an AODV pure ad hoc network through guard nodes. Elsevier Computer communications31(1796-1802).

Kurosawa, S. *et al*., 2006.―Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method,‖ Proc. Int'l. J. Network Sec.

Marti, S., T.J. Giuli, K. Lai, M. Baker, 2000. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. Paper presented at the 6th annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, 6-11.

Medadian, M., M.H. yektaie and A.M. Rehmani, 2009. Combat with blackhole attack in aodv routing protocol in MANETs,Proc.IEEE Asian himalayas International conference on Internet.

Ming-Yang Su, 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection system.Computer communication 34(107-117)in Elsevier Publications.

Mohana priya, M., Ilango krishnamurthi, 2014. Modified DSR protocol for detection and removal of selective black hole attack in MANET.Computers and Electrical Engineering40(201)5M. Asaka, A. Taguchi, and S. Goto,*et al*,1999-538 in Elsevier Publication.

Murty, M.S., M.V. Das, 2011. Performance Evaluation of MANET Routing Protocols using Reference Point Group Mobility and Random Waypoint Models. International Journal of Ad hoc, Sensor & Ubiquitous Computing, 2(1): 33–43. doi:10.1Da Zhang,Chai Kiat Yeo,20115/2008/860364.

Nidal naseer, Yungfeng chen, 2007. Enhanced Intrusion detection system for discovering malicious node in mobile ad hoc networks.IEEE communication society subject matter experts for publication in the ICC proceedings.

Padilla, E., N. Schenbruck, P. Maritini, m. Jhanke and J. Tolle, 2007. Detecting black hole attack in tactical MANRT using topology graph,Proc IEEE conference on local computer network.

Perkins, C., E. Belding-Royer and S. Das, 2003.―Ad Hoc Ondemand Distance Vector (AODV) Routing,‖ IETFRFC 561.

Ricardo Puttini, Jean-Marc percher, Ludovic Me and Rafael de sousa, 2004. Afully distributed IDS for MANET.Computer and communications proceedings ISCConIEEE.

Robert mitchell An intrusion detection model. In IEEE Transactions on software engineering, Vol. SE-13, NO.2,pages,Ing-ray chen(2014),F.T.seng,L.chou,C.chou(2011)2– F.T.seng,L.chou,C.chou(2011) 2. IEEE,1987.

Robert mitchell,Ing-ray chen, 2014. A Survey of intrusion detection in wireless network applications.Computer communications 42(2014) 1-F.T.seng,L.chou,C.chou(2011) in Elsevier publication.

Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, 2003. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks.

Seng, F.T., L.chou, C. chou, 2011. A survey of black hole attack in wireless mobile ad hoc networks, Journal on human centric computing and information sciences, springer, 1(4): 1-16.

Serigo Marti, T.J. Giuli, Kevin lai and Mary baker, 2000. Mitigating routing misbehaviour in mobile ad hoc networks.Proceeding Mobicom ’00 on the 6th annual international conference on mobile computing and networking in ACM publication.

Tseng, Y-C., J-R. Jiang, J-H. Lee, 2004. Secure Bootstrapping and Routing in an IPv6-based Ad Hoc Network. Journal of Internet Technology 5(2): 1F.T.seng,L.chou,C.chou(2011) –1M. Asaka, A. Taguchi, and S. Goto,*et al*,1999.

Umang, S., B.V.R. Reddy, M.N. Hoda, 2010. Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption. IET Communications 4(17): 2084-2094. doi: 10.1049/ietcom. 2009.0616.

Wu, B., J. Chen, J. Wu, M. Cardei, 2007. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In: Xiao Y, Shen X, Du D-Z (eds) Wireless Network Security. on Signals and Communication Technology. Springer, New York.

Yang, S-J., Y-C. Lin, 2009. Static and Dynamic RED Tuning for TCP Performance on the Mobile Ad Hoc Networks. Journal of Internet Technology, 10(1): 13–H. Debar, M. Dacier, and A. Wespi,*et al* 1998.

Yang, H., H. Lou, F. Ye, S. Lu, L. Zhang, 2004. Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications., 11(1): 38–47. doi: 10.1109/MWC.2004.1X.Y.Zhang,Y.Sekiya andY.wakahara,*et al* 20099716.

Yuvaraj singh, Sanjay kumar jena, 2011. Intrusion detection system for detecting mallicious nodes in mobile ad hoc networks.International conference on parallel,Distributed computing technologies and applications.

Zhang, Chai Kiat Yeo, 2011. Distributed court system for intrusion detection in mobile ad hoc networks.Elsevier in Computer and security M. Asaka, A. Taguchi, and S. Goto, *et al*, 1999(555-570).

Zhang, X.Y., Y. Sekiya and Y. wakahara, 2009. Proposal of a method to detect black hole attack in MANETs,IEEE International Symposium on autonomus decentralized system ISADS.

Zhou, L., H-C. Chao, 2011. Multimedia Traffic Security Architecture for the Internet of Things. IEEE Network M.Medadian, M.H.yektaie and A.M.Rehmani, (3): 29-34. doi: 10.1109/MNET.2011.5772059.