ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Securing MANETs using Cooperative Bait Detection System

[1]Nisha Soms, [3]Ms. C.S.Nithyapriya,[2]Dr.P.Malathi

[1]Assistant Professor(Sr.Gr.), [3]PG Scholar,[2]Professor

[1]Sri Ramakrishna Institute of Technology,[3,2]Bharathiyar Institute of Engineering for Women

[1]Pachapalayam,Coimabatore-10,[3,2]Deviyakurichi, Attur TK

nishasoms.cse@srit.org,csnithya93@gmail.com ,pmalathi2004@yahoo.co.in

***Abstract*—The advancement in the fields of the network has leaded the way for many wireless networks. Mobile ad hoc networks are continuously self- configuring, infrastructure less network. Each device in the MANETs is free to move independently in any direction. This continuously changing topology of the network leads to many attacks and the presence of malicious nodes. The main challenge is to detect the attack in the network and prevent them from affecting the network. Many of the research was done on prevention and removal of only two attacks as black hole and grey hole but still there are existence of other important most common attacks like wormhole and byzantine which are not proposed. The various applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations. Therefore the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network. A cooperative bait detection approach is given to prevent the collaborative black hole attacks with higher performance metrics and ensures safe network.**

***Index Terms*— Black Hole, Byzantine Attack,Collaborative Blackhole, Grey Hole, Mobile Ad hoc Networks, Wormhole Attack**

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a collection of mobile node connected through wireless links. In MANET all nodes are connected with the nodes near in communication range. It is a self-configuring network of mobile routers connected by wireless links with no access point. Every mobile device in a network is autonomous. MANET shares the wireless medium and the topology of the network changes erratically and dynamically. The structure of a MANET may vary from highly power-constrained small static network to a large-scale, highly dynamic mobile network [1]. These MANETs are two types i.e. closed and open. In a closed MANET, all mobile nodes cooperate with each other toward a common goal, whereas in an open MANET different mobile nodes with different goals share their resources in order to ensure global connectivity. An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology. In a MANET wireless transmission, the maximum energy consumed by the mobile nodes and as such when a selfish node refuses to forward data packets to other nodes the energy requirement. There are currently three main routing protocols for ad hoc networks, Destination Sequenced Distance Vector routing (DSDV), Dynamic Source Routing (DSR) and AODV [2].

DSR is an on-demand routing protocol and it maintains a route cache, which leads to memory overhead. DSR has a higher overhead as each packet carries the complete route, and does not support multicast. In DSDV, each mobile node in the network maintains a routing table with entries for every possible destination node, and the number of hops to reach them. The routing table is periodically updated for every

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

change in the network to maintain consistency. This involves frequent route update broadcasts. DSDV is inefficient because as the network grows the overhead grows as O(n2) [1].AODV (Ad hoc On-Demand Distance Vector) is a reactive routing protocol composed of two modules namely Route discovery module: To send data to a given destination D, the source node S consults its routing table. If it finds a valid entry (a route) towards this destination D, it uses it immediately, else it launches a route discovery procedure, which consists in broadcasting, by the source node S, a route request (RREQ) message (containing amongst other information: destination's address, destination's sequence number) towards neighbors. It is a source initiated on-demand routing protocol. Then the Route maintenance module: AODV uses Hello messages to maintain the connectivity between nodes. Each node periodically sends a Hello message to these neighbors and awaits Hello messages on behalf of these neighbors. If Hello messages are exchanged in the two directions, a symmetrical link between nodes is always maintained if no link interrupt occurs. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself. The destination node or the intermediate node with a fresh enough route to the destination node, unicasts the Route Response (RREP) message to the neighboring node from which it received the RREQ.

An intermediate node makes an entry for the neighboring node from which it received the RREP, and then forwards the RREP in the reverse direction. On receiving the RREP, the source node updates its routing table with an entry for the destination node, and the node from which it received the RREP. The source node starts routing the data packet to the destination node through the neighboring node that first responded with an RREP. There are several types of attacks in mobile ad hoc networks[8]. The attacks in MANET can be briefly classified into two categories: external attacks and internal attacks. The two important type of attacks are black hole and grey hole attack. They are qualified passive ones, if they are limited to the listening of the network traffic to take note, or active if the traffic is modified by the intruder. A black hole is a malicious node that falsely replies for any Route Requests (RREQ) without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack.

In this paper, a mechanism called Cooperative Bait Detection Scheme (CBDS) is presented that effectively detects the malicious nodes that attempt to launch collaborative blackhole attacks. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique.

II. RELATED WORK

Many researches have investigated the problems of the different types of attack and the methods to detect and prevent them. Jian et.al [1] proposes a scheme to preventing and defending the malicious nodes that launches the grey and black holes. It resolves the issue by designing a mechanism based upon the dynamic source routing (DSR) algorithm. The scheme uses both the advantages of proactive and reactive architectures.

The two main processes of dynamic source routing involved are route discovery and route maintenance. The destination nodes depend upon the collected routing information among the packets in order to send a reply RRREP message. Here the address of the adjacent node is used as the bait destination address that helps to detect the malicious node using reverse tracing technique.

Vishnu et Al [2] proposes a protocol for detection and removal of the networking Black/Grey holes with the complete mechanism for the malicious nodes with those attacks. The proposed mechanism steps as follows. First, a trusted node of network is being established with the AODV protocol.

The restricted (unused) IP addresses of the nodes are being obtained by the source node of the network. When the source node starts to transmit, it performs two main actions as select the destination node by sending RREQ in the network and also finds the restricted nodes. If a malicious node finds the RREQ, it replies with RREP of the restricted (unused) nodes.

Then the source node starts the mechanism for detection and removal of the malicious nodes present in the network.

Deng et al[3] proposed a mechanism to defend against the black hole attack in the networking. When a node receives the request packet RREP from the source node. If the next hop either does not have a link to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. This technique does not work when the malicious nodes cooperate with each other.

S.Ramaswamy et al[4] presented an algorithm to prevent the co-operative black hole attacks in ad hoc network. This algorithm is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attacks. Besides, due to intensive cross checking, the algorithm takes more time to complete, even when the network is not under attack.

The two properties of black hole are first it exploits the route to the destination node. Second, the node consumes the intercepted packets with the source and destination. To do the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

task it invokes the data with the Data Routing Information Table which contains the information about the transaction of the nodes from and through the defined network.

S.Banerjee et al [5] has also proposed an algorithm for detection & removal of Black/Gray Holes. According to their algorithm instead of sending the total data traffic at once, they divide it into small sized blocks, in the hope that the malicious nodes can be detected& removed in between transmission. The detection mechanism follows two types of schemes called proactive and reactive.

1) *Proactive detection scheme:*

These schemes have to constantly detect or monitor the nearby nodes in the network. Here, an overhead for the detection process is being created. This type of scheme helps us to prevent an attack in the initial stage.

2) *Reactive detection scheme:*

These types of schemes will be triggered only if the destination node detects a significant drop in the packet delivery ratio.

Based on the two defense phases the detection mechanism adapts the triggers to prevent the network. These have an advantage similar for the system and those advantages are being merged together to obtain the results for the system. The initial stage monitoring is triggered with the proactive with the overhead and when there is fall in the packet delivery ratio the reactive phase is triggered each situation is analyzed and the schemes are triggered accordingly.

III. PROPOSED SYSTEM

This paper proposes a detection system called Cooperative Bait Detection System (CBDS), which is designed to detect the malicious black hole in the network. In MANET, the source node selects the adjacent nodes to transfer the packets to the selected destination node. This approach will have a bait node that selects the adjacent nodes to detect for the malicious nodes in the network. When a significant drop in the malicious node is encountered it triggers an alarm according with the reactive scheme to the system. Hence, the detection mechanism is initialized that checks for the malicious black hole in the network. This system also merges the advantage of the proactive system that could help to find the malicious node in the initial stage. The malicious node could be anywhere in the network causing a packet drop and delay in transmission of the packets. The most common attacks that occur in MANETs are black hole and grey hole. It is concluded that several authors have provided the approach for detection of individual malicious attack also many mechanism just black lists the malicious node. The effectiveness of these approaches become weak when the malicious node collide together to initiate a collaborative attack which may cause damage to the network. Hence an approach that helps the detection and prevention of the collaborative attacks should be provided. This approach will find the alternative list for the safe transmission of the packets between the nodes with the neighbor nodes in the network. The performance metrics ensures the feasibility and accuracy of the network.

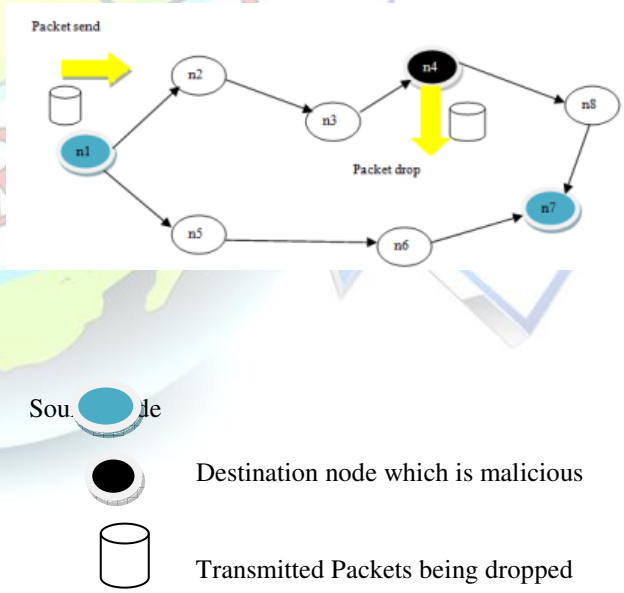

Fig 1.1 Blackhole attack in MANET

The cooperative bait detection scheme consists of three steps: 1) The initial bait step, 2) Reverse tracing step and 3) Shifted to Reactive defense phase.

A. *Initial Bait Step*

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

The goal of the bait phase is to entice a malicious node to send a reply RREP by sending the bait RREQ that it has used to advertise itself as having the shortest path to the node that detains the packets that were converted. To achieve this goal, the following method is designed to generate the destination address of the bait RREQ'. The source node stochastically selects an adjacent node, i.e., nr, within its one-hop neighborhood nodes and cooperates with this node by taking its address as the destination address of the bait RREQ. Since each baiting is done stochastically and the adjacent node would be changed if the node moved, the bait would not remain unchanged. The bait phase is activated whenever the bait RREQ, is sent prior to seeking the initial routing path. The follow-up bait phase analysis procedures are as follows. First, if the n r node had not launched a black hole attack, then after the source node had sent out the RREQ , there would be other nodes' reply RREP in addition to that of the nr node. This indicates that the malicious node existed in the reply routing. Therefore, the reverse tracing program in the next step would be initiated in order to detect this route. If only the nr node had sent the reply RREP, it means that there was no other malicious node present in the network and that the CBDS had initiated the DSR route discovery phase. Second, if nr was the malicious node of the black hole attack, then after the source node had sent the RREQ, there nodes (in addition to the nr node) would have also sent reply RREPs. This would indicate that malicious nodes existed in the reply route. In this case, the reverse tracing program in the next step would be initiated to detect this route. If nr deliberately gave no reply RREP, it would be directly listed on the black hole list by the source node. If only the nr node had sent a reply RREP, it would mean that there was no other malicious node in the network, except the route that nr had provided; in this case, the route discovery phase of DSR will be started. The route that nr provides will not be listed in the choices provided to the route discovery phase.

B. Reverse Tracing Step

The reverse tracing program is used to detect the behaviors of malicious nodes through the route reply to the RREQ, message. If a malicious node has received the RREQ, it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the dubious path information and the temporarily trusted zone in the route. It should be emphasized that the CBDS is able to detect more than one malicious node simultaneously when these nodes send reply RREPs.

Indeed, when a malicious node, for example, n_m, replies with a false RREP, an address list P = {n_1, . . .n_k, . . . n_m, . . . n_r} is recorded in the RREP. If node n_k receives the RREP, it will separate the P list by the destination address n_1 of the RREP in the IP field and get the address list k = {n1, . . . nk}, where krepresents the route information from source node $n_1$to destination node n_k. Then, node n_k will determine the differences between the address list P = {n_1, . . .n_k, . . . n_m, . . . …n_r} recorded in the RREP and list k = {n_1, . . . n_k},. Consequently, we get

K_k=P- K_k= {$n_{(k+1)}$,.....n_m ,.....n_r }

where$K_k$represents the route information to the destination node (recorded after node n_k). The operation result of $K_k$is stored in the RREP's "Reserved field" and then reverted to the source node, which would receive the RREP and the address list $K_k$of the nodes that received the RREP. To avoid interference by malicious nodes and to ensure that K_k,does not come from malicious nodes, if node n_k received the RREP, it will compare:

1) The source address in the IP fields of the RREP;
2) The next hop of nk in the = {n_1, . . .n_k, . . . n_m, . . . n_r};
3) One hop of n_k.

If A is not the same with B and C, then the received $K_k$can perform a forward back. Otherwise, n_k should just forward back the K_k that was produced by it.

Given that a malicious node would reply the RREP to every RREQ, nodes that are present in a route before this action happened are assumed to be trusted. The set difference operation of P and S is conducted to acquire a temporarily trusted set T, i.e.,

$$T = P - S$$

To confirm that the malicious node is in set S, the source node would send the test packets to this route and would send the recheck message to the second node toward the last node in T. This requires that the node had entered a promiscuous mode in order to listen to which node the last node in T sent the packets to and fed the result back to the source node. The source node would then store the node in a black hole list and broadcast the alarm packets through the network to inform all other nodes to terminate their operation with this node. If the last node had dropped the packets instead of diverting them, the source node would store it in the black hole list.

B. SHIFTED TO REACTIVE DEFENSE PHASE

After the above initial proactive defense (steps A and B), the DSR route discovery process is activated. When the route is established and if at the destination it is found that the packet delivery ratio significantly falls to the threshold, the detection scheme would be triggered again to detect for continuous maintenance and real-time reaction efficiency. The threshold is a varying value in the range [85%, 95%] that can be adjusted according to the current network efficiency. The initial threshold value is set to 90%. We have designed a dynamic threshold algorithm that controls the time when the packet delivery ratio falls under the same threshold. If the descending time is shortened, it means that the malicious nodes are still present in the network. In that case, the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

threshold should be adjusted upward. Otherwise, the threshold will be lowered. The operations of the CBDS are captured. It should be noticed that the CBDS offers the possibility to obtain the dubious path information of malicious nodes as well as that of trusted nodes; thereby, it can identify the trusted zone by simply looking at the malicious nodes reply to every RREP. In addition, the CBDS is capable of observing whether a malicious node would drop the packets or not. As a result, the proportion of dropped packets is disregarded, and malicious nodes launching a gray hole attack would be detected by the CBDS the same way as those launching black hole attacks are detected.

IV. PERFORMANCE METRICS

The Performance of the CBDS system could be estimated by the following metrics as:

1) Packet Delivery Ratio**:** This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source. Here, $pktd_i$ is the number of packets received by the destination node in the ith application, and $pkts_i$ is the number of packets sent by the source node in the ith application. The average packet delivery ratio of the application traffic n, which is denoted by PDR, is obtained as

$$PDR = \frac{1}{n}\sum_{i=1}^{n}\frac{pktd_i}{pkts_i}.$$

2) Routing Overhead**:** This metric represents the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. Here, cpk_i is the number of control packets transmitted in the ith application traffic, and pkt_i is the number of data packets transmitted in the ith application traffic. The average routing overhead of the application traffic n, which is denoted by RO, is obtained as

$$RO = \frac{1}{n}\sum_{i=1}^{n}\frac{cpk_i}{pkt_i}.$$

3) Throughput:This is defined as the total amount of data(b_i) that the destination receives them from the source divided by the time (t_i) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. The throughput of the application traffic n, which is denoted by T, is obtained as

$$T = \frac{1}{n}\sum_{i=1}^{n}\frac{b_i}{t_i}.$$

The system is compared along with the metrics to enhance the feasibility and correctness of the packets being delivered. The system ensures the secure transmission of the packets to the destination by selecting the path that is safe with the hop latency of the neighbor nodes. When a malicious node is detected the system could black list the node and do not allow any transmission through the black listed nodes. Hence a secure path with the neighbor nodes is selected and the new path is used to transmit the packets safely.

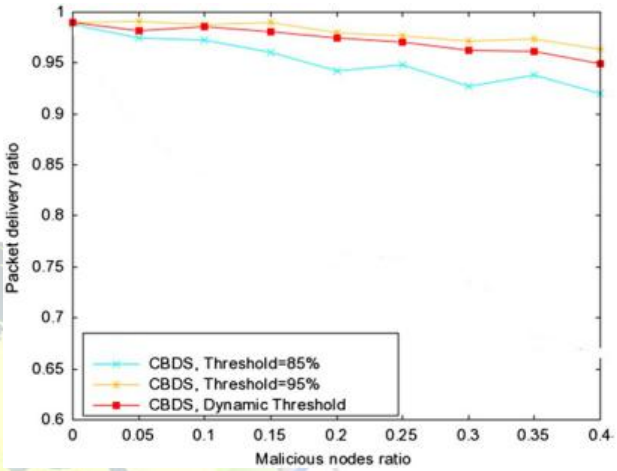

Fig 1.2 Packet delivery ratio metric

First the system is compared with the ratio of the packet being delivered with the source and the destination. The network is set with different thresholds to detect the average attack in the network. A threshold of 85% and 95% is given to the nodes. The speed of the network is set as 30 m/s. From the graph it is evident that the probability of the black hole attack increases with the increase in the threshold value given to the network. This is referred to as changing the mobility of the nodes according to the fixed variability.

V. CONCLUSION

The proposed mechanism known as the CBDS for detecting malicious nodes in MANETs detects the gray/collaborative blackhole attacks. The presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations. The simulation results revealed that the CBDS outperforms the 2ACK, and BFTR schemes, that detects the malicious node and changes its path by negotiating the particular node and forms a new list that ensures the secure transaction of the packets. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network. As future work, we intend to the other types of attacks like wormhole attacks to ensure more security of the MANET and check for the feasibility and performance of the nodes in MANET.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

REFERENCES

[1] Jian-Ming,po-chunTsou,IsaacWoungang,Han-Chieh Chao and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", Member,IEEE.
[2] K.Vishnu and A.J paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks", in Proc,6thAnnu.Intl.conf.
[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.
[4] Sanjay Ramaswamy, Huirong Fu, ManoharSreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada,USA, pp. 570-575.
[5] SukulaBanarjee "Detection / Removal 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.
[6] G. Bella, G. Costantino, S. Riccobene, Managing reputation over manets, in: Fourth International Conference on Information Assurance and Security, Naples, Italy, 2008, pp. 255–260.
[7] R.Balakrishna, U.RajeswarRao ,N.Geethanjali, "detection of routing misbehavior in mobile ad hoc networks", journal of networks, vol. 3, no. 5, may2008.
[8] LathaTamilselvan, Dr.V.Sankaranarayanan, "prevention of co-operative black hole attack in MANETs" journal of networks, vol.3, may 2008.
[9] RajendraV.Boppana, Xu Su, "On the Effectiveness of monitoring for intrusion detection in Mobile Ad Hoc Networks", journal of computer science, vol.7, 2009.
[10] Saju P John, Samuel Philip, "Self organized key management with trusted certificate exchange in MANET", vol.6, December 2014.
[11] C. Chang, Y. Wang, and H. Chao, "An efficient Mesh-based core multicast routing protocol on MANETs," J. Internet Technol., vol. 8, no. 2, pp. 229– 239, Apr. 2007.
[12] A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.
[13] Jian-Ming,po-chunTsou,I Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehav-ior in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265
[14] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowl-edgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.
[15] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.
[16] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009.
[17] SudipMisra, Isaac woungang, Subhas Chandra Misra, "Guide to wireless Ad Hoc Networks", Springer International,2011