RESEARCH ARTICLE OPEN ACCESS

Link Reliability based Detection and Predecessor base Route Establishment for Prevention of Wormhole Attack

Nansi Jain, Yogendra Kumar Jain
Computer Science and Engineering Deptt. Samrat Ashok Technological Institute Vidisha, India
Computer Science and Engineering Deptt. Samrat Ashok Technological Institute Vidisha, India

ABSTRACT
Mobile Ad hoc Network (MANET) is consists of mobile hosts or sensor nodes proficient of functioning in absence of infrastructure. Such networks should be capable of self forming, self organizing, self managing, self recovering, and able to operate under dynamic conditions. The multi-hop communication phenomenon is used to sending information to receiver. To attain this, each mobile node depends on its neighbor or range node to forward the data packet to the destination. In fact, most of previous studies on MANET have implicitly assumed that nodes are cooperative such as node cooperation becomes a very important issue in MANET. The attacker in dynamic network are easily affected the routing performance and data receiving ratio is affected as compared to normal performance of network as well as dropping of data is enhanced. The packets percentage is degrades is the confirmation of attacker misbehavior. The characteristics of wormhole attack is to making the tunnel and reply the positive acknowledgement of destination at time of route request and drop all the data deliver through tunnel. The attacker is identified by the past and current data receiving and forwarding in MANET. The proposed IPS (Intrusion Detection and Prevention System) provides the security on the basis of link reliability. In this work, we proposed new link reliability based security through Predecessor based Route Establishment of detecting routing misbehavior of wormhole attack for prevention in MANET. The attacker is blocked through the broadcasting scheme used by proposed prevention scheme from their actual identification to neighbors. The security provider nodes are blocking the communication of attacker and provide the secure communication among the mobile nodes. The performance of proposed scheme is evaluated through performance metrics like PDR and throughput.

Keywords: WSN, Routing, Malicious, wormhole, Link Reliability, IPS.

I. INTRODUCTION

There are two types of wireless networks, i.e. infrastructure based wireless networks and wireless ad hoc networks. An Ad hoc mobile network is deliberated to trounce the natural limitation of wired backbone networks and infrastructure based wireless networks. The network is a collection of mobile nodes that uses a wireless channel and dynamically forming a temporary network topology without the existence of network infrastructure or centralized administration [1]. The wireless and wired networks are not possible to build rapidly in critical circumstances like heavy flooding earthquake etc. [1]. The main advantage of MANET is to easily established at anywhere for communication to nest node or sensor. Due to the restriction of transmission range, each mobile node can only communicate with neighbouring nodes within its radio coverage area besides, forwarding packets for other nodes; it also acts as a router for taking routing decisions and forwarding packets to destination or other neighbour. Mobile Ad hoc networks are also called multi-hop wireless networks because any message or data transmitted from a source node to a destination node not possible directly communicate. It may also possible through many intermediate nodes, which requires multiple interconnected hops [1, 2]. The system may operate in isolation or may have gateways connected with a fixed network. In the latter mode, it is typically envisioned as a sub network connected to a fixed network. The mobile devices used in ad hoc networks could include an evolution of current cell phones, PDAs, or laptops equipped with wireless interfaces. In a MANET, each mobile node is equipped with a wireless transmitter and receiver using antennas. Nodes can communicate directly with other nodes within their wireless transmission range. However, wireless links have significantly lower capacity and transmission range than their hardwired counterparts due to effects such as signal fading, noise and limited battery power. Attacks on MANET are classified as Active and Passive attacks [3, 4], passive attacks are not dangerous, if the delivering data is important than its security, because it does not affects the normal operation of MANET. While, active attacks affecting the normal operation of MANET In several ways. This research work is focusing on initiatives which make MANET survives against wormhole attack [4].

Malicious node causes packet dropping, false routing and etc. Effects of malicious nodes are given below:

- Malicious node reduces the network connectivity in MANETs.
- The result is defragmented networks, isolated nodes, and drastically reduced network performance.
- Their main intention is in any cost affected the routing performance of dynamic network
- Launch misbehavior when sender is sending data replaying, reordering or/and dropping packets from time to time, and even by sending fake routing messages.

II. ROUTING PROTOCOLS IN MANET

In dynamic network i.e. MANET, the network topology are frequently changes that are the cause of link breakage and possibility of retransmission are enhanced. The direct connection in between sender and receiver is hardly ever possible. The connections are created as multi-hop till the destination is not found. The malicious nodes in this open network is easily affected the actual data delivery. The routing protocol play a important role at network layer for data accepting and forwarding through each router or node but these routing protocols are not able to protect the network from attacker. The data is sending by sender and accepted by receiver and in this procedure routing strategy is very important part of communication [5, 6]. For connecting to destination and data delivery, routing protocol is necessary for routing the data in between sender to receiver. Every routing protocol has different routing strategy for connection establishment, but it has same strategy i. e. select the shortest path in between sender and receiver. The shortest path is decided on the basis of minimum hop count value in MANET. The classifications of routing protocols in MANET are as follows:-

(A) Proactive Routing Protocol

The proactive routing protocols are also called as table driven routing protocol and these routing protocols are maintaining the routing information of each node that are participating in routing procedure. In Mobile Ad hoc network the topology in network is changes by that the overhead to maintain the information of each and every node is very difficult and required large amount of memory for storing routing information in network. In ad hoc network, if the nodes are moves at slow speed then that protocol is suppose to be better for communication. The example of proactive routing protocol is DSDV routing protocol.

(B) Reactive Routing Protocol

The Reactive routing protocols are also called as on demand routing protocol and these routing protocols are maintaining the routing information on the basis of requirement of request receives by the neighbour. There is no routing information is stored of each node that are participating in routing procedure. In Mobile Ad hoc network, topology in network is changes by that the overhead to maintain the information of each and every node is not needed to maintain. In ad hoc network, if the nodes are moves at random speed then that protocol is supposes to be better for communication. The example of reactive routing protocol is AODV routing protocol.

(C) Hybrid Routing Protocol

Since proactive and reactive protocols each work best in oppositely different scenarios, hybrid method uses both. It is used to find a balance between both protocols. Proactive operations are restricted to small domain, whereas, reactive protocols are used for locating nodes outside those domains.

III. LITERATURE SURVEY

This section covers previous work in the field of security proposed by different researchers. The prominent research work in field of dynamic network by the different researchers is as given below:

Waseem et al proposed detection and prevention of the network from wormhole attacks, and also given an enhanced version of AODV hello packets [7]. They considered some assumption such as clock time is synchronized and used during neighbor discovery. Neighbor nodes respond with appending Hello massage with present received time and reply. The route information is stored in source, destination and intermediate nodes. An attacker tunnels a request packet delivery to the destination node without hop-count value and stop route discovery.

Hongsong et al proposed security scheme to enhance security and reliability in sensor network [8]. Trust can be interpreted as belief, reputation, probability and trustworthiness. Trust routing reflects the trustworthy degree of routing path. In sensor network, in addition to the traditional hop count, routing trustworthiness is related to many factors, such as node's residual energy node's attack behaviour. They have shown that each factor is assigned one agent to monitor the varieties, trust routing agent integrates the factors into trust routing value, the trust routing will be more objective and trustworthy. Because the different metrics of different factors, a unified trust routing metric is necessary.

Suraj Thawani et al proposed security scheme by that Sybil node can be detect by the default value of RSS (Receive Signal Strength) and Threshold value [9]. If the value rise from actual value, then it is

Sybil node. These Sybil nodes are checked by the neighboring nodes and it can be protected by verifying token through master node. Temporarily Ordered Routing Protocol (TORA) is a distributed routing algorithm that is based on a family of link reversal algorithms. Sybil attack is an injurious attack in MANETs, attacker makes the multiple identities in the network as a malicious node with the several address. In this each nodes in the network has given unique address then also it make fake identities from the unique addresses in the network to collect the private information from the nodes.

Xiong Kail et al proposed the FP-Growth according concept in the AODV route table information for reducing black hole attack detection times [5]. The algorithm mines a rank sequence, which is not sensitive to the noise interference. Particularly, when the wireless environment becomes stochastic, the detection of rank sequence is better than the detection of distribution. In general, the behavior of malicious node will affect its neighbors. So, a detection of rank changed outcome has a large probability to be a suspicious nodes set.

Kashif Saghar et al focused on one such attack called hello flood attack [9]. Some WSN routing protocols require the nodes to announce themselves to neighbor nodes using a 'Hello' message. This message enables the receiver nodes in neighborhood, which can hear this message, to assume that the sender is within their radio range. This is a simple way of initializing a sensor network. However, there is a problem in this simple mechanism as this leads to hello flood attacks. In this type of DoS attack, a laptop-class attacker broadcasts the routing/other information with large enough transmission power to convince many or all the WSN nodes that the attacker is a genuine neighbor. The hello flood attack thus causes unidirectional links between the attacker and the legitimate nodes.

IV. PROPOSED WORK

Mobile Ad hoc network is a vulnerable network because varieties of attacks in dynamic environment and all those attacks capture the data packets or dropped the data and reduce the network services. In our proposed work, we detect and prevent wormhole attack under mobile ad hoc network. Wormhole attack is an active attack which contains at least two wormhole nodes and connected each other via wireless communication where attacker receives data packets from sender and forward to connected attacker node that create tunnel between those wormhole nodes and partially drop the data or capture the data. Wormhole attack detection and prevention is not an easy task because network is spread in wide area and therefore we proposed IPS (Intrusion Detection and Prevention System) which is link reliability based detection and predecessor base route establishment for wormhole prevention in MANET. In this methodology, initially use the routing protocol AODV and broadcast the routing packet and established the route from source to destination and then sends the data packet to the destination. If wormhole nodes present during communication, then the packets are tunnel in between those wormhole nodes. In our proposed mechanism, defensive node (IPS node) watches the established link and calculate packet delivery ratio between each connective link at every pause time, if packet delivery ratio is lower than the 50 percent than get the reason why the performance was decreased, because packet dropped by number of different reason such as route error, MAC error, queue drop and attacker drop. When the drop reason identified as a loop based or tunnelled in attacker node, then block the tunnel nodes and that detected link marked a wormhole link. After the detection of wormhole link, IPS node broadcast the wormhole node information in the network, so all the mobile node get alert and shall not use the attacker link. Those nodes which send data packet through the attacker link, IPS node break the connection from predecessor of wormhole nodes and established the new connection from receiver node using local route repair mechanism, which minimized the overhead of security and provide secure communication between sender and receiver nodes.

Proposed Algorithm:

This section describes approach of our proposed method to detect and protect wormhole attack under AODV routing. In the input section of proposed algorithm, all the required parameter initialize and output achieve through given routine based approach. Given algorithm is combined approach of detection and prevention of wormhole attack.

Algorithm: Wormhole node Detection and Prevention

Input: M: Mobile nodes
S: Sender nodes
R: Receiver Nodes
W1, W2: Wormhole nodes
IPS: set of preventer node
Antenna: Omni Antenna
pdr: packet delivery ratio
rr: radio range
AODV: routing packets
I: set of intermediate nodes
T*: pointer to predecessor
L: set of link between i_1, i_2 node

Output: wormhole percentage, throughput, PDR, overhead and UDP analysis

Routine:
Broadcast-route (AODV, S, R, rr)
While (I == in rr) **do**

I← receives routing packets
I← update rtable
For each I in range , P watch the I node and its link
While S ≠ R **do**
Calculate Trust of I: (forward/receives)*100
If (Trust < 50) **Then**
Identifies W1, W2 nodes
Identifies reason of drop
If (reason == wormhole) **Then**
Block link
T*← point predecessor node
T broadcast route packet & eliminate W1, W2
Established new path S to R
End if
End if
End do
If (R== S) **then**
Send Ack to T node
Call data-pkt()
Else
R not in zone
End if
End do
Data-pkt(S,R,pkt)
Count =1
If path is available **then**
All node in link i_1, i_2 watch by P
End if
While pkt incoming i_1 to i_2**do**
If i_2 receives && pkt-forward ≠ true **then**
Decrease-trust = i_2-old-trust – (forward/receives)
i_2← new-trust-level
if (i_2 pdr < 50)
call local repair(S,R,AODV-local-R)
Else
Increase-trust = i_2-old-trust + (forward/receives)
i_2← new-trust-level
End if
all P calculate separately trust level of i_1 and i_2 link
P send trust report to M-2 node // eliminate w1, w2
S re established new path to R
End do

The proposed scheme is not only detecting the attack in dynamic network, but also applied prevention scheme on it. The proposed scheme identified the tunnel link in between sender and receiver and blocks that link for secure communication in MANET.

V. SIMULATION OVERVIEW

The simulation is done in NS-2 simulator [16]. The NS-2 is the freeware toll available in internet. Due to open source simulator the modification in experimental environment is easily possible. The scripting is written in TCL (Tool Command Language) language and the internal modules are built in C++ language, that's why also called OTCL (Object Oriented TCL). This simulator version is used NS 2.31. This is a freeware tool for simulating the scenarios of wired, wireless, sensor and Ad hoc network. The performance of three routing schemes i. e. Proactive Routing Protocol, Reactive Routing Protocol, and Hybrid Routing Protocol is compared through defined performance metrics with considered simulation parameters in this work.

Performance Parameter

In our simulation we apply network simulator-2 and analyse the behaviour of the network through following metrices:

- **Packet Delivery Ratio:** The ratio between the number of packets originated by the application layer CBR sources and the number of packets received by the CBR sink at the final destination.
- **Attacker Infection:** The attacker infection is measured in network by calculating the dropping percentage of packets through attacker only.
- **Packet Dropped:** The routers might fail to deliver or drop some packets or data, if they arrive when their buffer are already full. Some, none or all the packets or data might be dropped, depending on the state of the network, and it is impossible to determine what will happen in advance.
- **Routing Load:** The total number of routing packets transmitted during the simulation. For packets sent over multiple hops, each transmission of the packet or each hop counts.
- **UDP End Packets receiving and Loss:** The number of packets transfer from network layer to transport layer. The packets receiving as ratio of sending is provides the receiving and loss of packets.

Simulation Parameter

The simulation is performing in area of 1200*1200 meter area in 802.11 wireless IEEE standards. The propagation model is use Two ray ground propagation model. The reactive routing protocol AODV is used for routing. Some other simulator parameters are also considered such as Number of nodes, Routing protocol and traffic. The simulation environment is defined in table 1 (shown below).

Table 1: Simulation Parameter

Number of nodes	150
Dimension of simulated area	1200×1200
Routing Protocol	AODV
Work on Attacker	Wormhole
Simulation time (seconds)	100
Transport Layer	TCP ,UDP
Traffic type	CBR , FTP
Packet size (bytes)	1000

Number of traffic connections	20
Nodes Motion	Random
Nodes Maximum speed	30m/s

VI. SIMULATION RESULTS

In this section the simulation performance of normal AODV, trusted AOD (T-AODV), routes in presence of wormhole attacker and proposed IPS security scheme.

A. Overhead Analysis

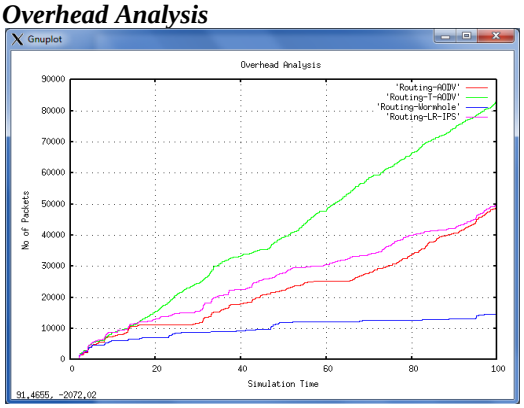

Fig.A: Routing Flooding Analysis

The routing overhead performance of normal AODV, Trusted AODV, Wormhole attack, and proposed link reliability based IPS scheme for securing MANET. The routing overhead performance of T-AODV is maximum. The performance of routing overhead is minimum in case of wormhole attacker but data packets receiving is minimum. That is the indication of performance degradation and malicious behavior. But in the case of proposed IPS routing overhead is in between T-AODV and wormhole attack.

B. PDR Analysis

In this graph, PDR performance of all four proposed protocol including proposed is presented and observed that the proposed IPS performance provides PDF performance 76% which is slightly better performance than the other methods.

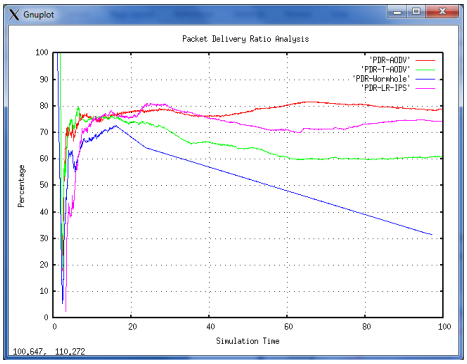

Fig.B: PDF Performance Analysis

C. Throughput Analysis

The throughput performance of all four protocols is shown in this graph. The packets receiving per unit of time is measured through throughput and the throughput of T-AODV is better but with more overhead. But, graph clearly shown that overall performance of proposed scheme in terms of throughput is improved.

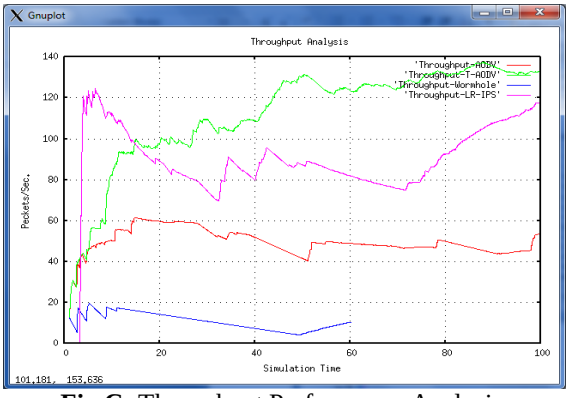

Fig.C: Throughput Performance Analysis

D. UDP End Transmission Analysis

The packets transmission at connection less transport layer protocol is in T-AODV is more. The next better performance is of proposed IPS. The rest of the methods shown poor performance. The attacker is not affected the sending of packets, although it affect the packets receiving.

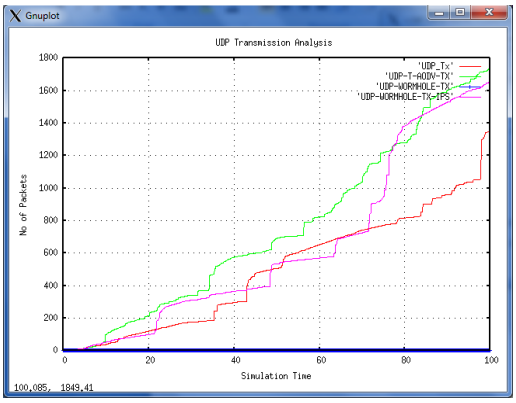

Fig.D: UDP Transmission Analysis

E. UDP End Transmission Analysis

The packets receiving performance of all protocols is evaluated in this graph and observed that the proposed IPS provides the highest receiving that clearly indicates better security scheme in MANET. The UDP performance is easily affected because of connection less mechanism. The only attacker performance is about negligible in term of packets receiving. The better and more packets receiving gives the better performance of network and our proposed IPS scheme provides better performance.

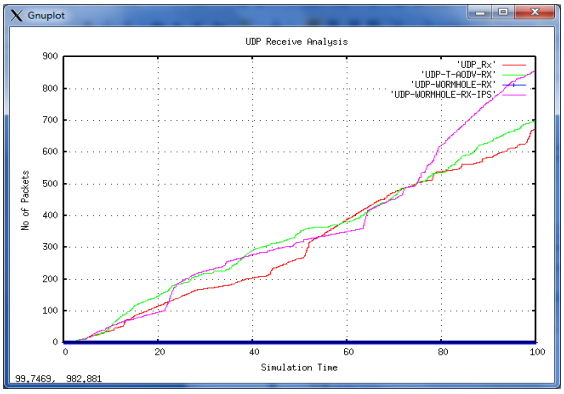

Fig.E: UDP Receiving Analysis

F. Wormhole Loss Analysis

The proposed scheme provides the secure communication in presence of IPS. In this graph packets drop percentage in presence of attacker is evaluated and observed at the end of simulation, the packets drop percentage in presence of attacker with the proposed scheme is 20%. The attacker infection in presence of IPS is zero that is the positive and strong effect of security scheme.

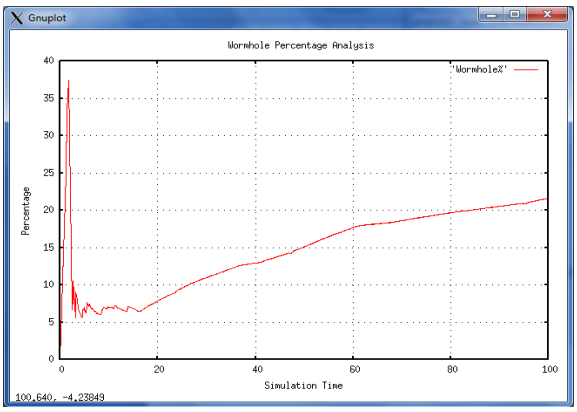

Fig.F: Attacker Loss Analysis

VII. CONCLUSION AND FUTURE WORK

The routing protocol are not able to handle the attacker misbehaviour because attacker is behaves like as normal node when the sender node is in call connection establishment procedure with receiver. The receiver is not known the attacker is generating the fake information of actual route to sender. Our proposed IPS (Intrusion Detection and Prevention System) is not only detecting the attacker but also prevent from attack. The sender is not known the reply is generated by wormhole attacker and it trusts the intermediate nodes and starts the data transmission.The proposed link reliability based security method against wormhole attack is not only detect the wormhole attacker but also prevent the network from it according to predecessor information of routing through nodes in dynamic network. The proposed scheme improves the routing performance and provides the secure communication. The attacker degrades the routing performance, because the PDR performance is less than 50. If the PDR is greater than 50, then the communication is secure. The information of attacker is broadcast to all the nodes that are participating in routing procedure and these nodes ignore the request of attacker. If node is identified again in the network as attacker, the existence of that existence of node is blocked in the network. The attacker infection is very harmful for MANET. By this the routing overhead, throughput and PDF are provides the negligible output but after applying proposed secure scheme the routing packets flooding is minimized with enhancement of performance of PDR and packets receiving. The performance of proposed security scheme is on upper side as compared to conventional routing methods.

In future, security scheme against vampire attack and Sybil attack can be investigated. The attacker identification may not be based on packet loss only but also based on resource consumption and multiple fake identities.

REFERENCES

[1] Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attsacks," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, 2013.

[2] R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah, and K. N. Qureshi, "Security Issues and Attacks in Wireless Sensor Network," World Applied Sciences Journal, Vol. 30, pp. 1224-1227, 2014.

[3] Y.A. Huang, W Lee,"Attack Analysis and Detection for Ad hoc Routing Protocols', Seventh International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Rivera, September 2004.

[4] B. Wu, J. M. Chen, J. Wu and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, Berlin, pp. 103-135, 2007.

[5] S. Giannoulis, C. Antonopoulos, E. Topalis, and S. Koubias, "ZRP versus DSR and TORA: A comprehensive survey on ZRP performance," presented at the 1 0th IEEE Conference on Emerging Technologies and Factory Automation (ETFA ' 05), pp. 1-8, 2005.

[6] Sree Ranga Raju, Kiran Runkana, Jitendranath Mungara, "ZRP versus AODV and DSR: A comprehensive study on ZRP performance", International Journal of Computer Applications (0975 – 8887) Volume 1– No12, 2010.

[7] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal,Abdul Hanan Abdullah and Kashif Naseer Qureshi, "Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks", IEEE International Conference on Smart Sensors and Application (ICSSA), 2015.
[8] Chen Hongsong, Han Zhi, Fu Zhongchuan, "Quantitative Trustworthy Evaluation Scheme for Trust Routing Scheme in Wireless Sensor Networks", IEEE Trustcom/BigDataSE/ISPA, 2015.
[9] Suraj Thawani, Hardik Upadhyay, "Securing TORA against Sybil Attack in MANETs",2015 1st International conference on futuristic trend in computational analysis and knowledge management (ABLAZE 2015), 475-478, 2015.
[10] Kashif Saghar, David Kendall, Ahmed Bouridane, "RAEED: A solution for Hello Flood Attack", Proceedings of IEEE 12th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 248-243, 13th – 17th January, 2015.
[11] Xiong Kail, Yin Mingyong, Li Wenkang, Jiang Hong, "A Rank Sequence Method for Detecting Blackhole Attack in Ad hoc Network", IEEE International Conference on Intelligent Computing and Internet of Things (IC1T), pp. 155-159, 2015.
[12] http://www.isi.edu/nsnam/ns