Master Aodv Algorithm to Detect and Prevent Worm-Hole Attack in Manet

K.Madhuri , N.Kasiviswanath

Abstract*: *Network is an assemblage of communicating terminals or nodes. Networks can be Computer Networks, Mobile Networks, and other type of networks. Networks are classified depending on many technical parameters , like Analog , Digital, Personal Area Networks(PAN) , Local Area Networks(LAN), Metropolitan Area networks(MAN) Virtual Private Networks(VPN) etc. In this work, we restrict ourselves to the study of problems of Mobile Networks routing. Due to the absence of secure boundaries, the MANETs are prone to attacks of various kinds, from any node in the network, by targeting several additional node(s) in the network which is within the radio range. Outbreaks of various kinds like inactive snooping, active snooping, and outflow of furtive data, information altering, message repetition, message exploitation, as well as denial of service can attack the mobile ad hoc network, and make it hard for the nodes to refuse the attacks in the network. Safety is a stimulating effort in ad hoc networks. Considerate promising methods of attacks are the leading stage for emerging better safety resolutions. The existence of mischievous nodes will be detrimental to the presentation as well as consistency of the network. Absence of any method for attack detection makes an ad-hoc network more susceptible compared to wired network.

Keywords*: *MANET, Routing, Attacks, Security

I. INTRODUCTION

Mobile Networks [1] created for communication between users are of various types and use different technologies like GSM, LTE, CDMA etc. These networks can be Fixed or Mobile. The linked connections between the components could be onfixed or temporary / Ad-Hoc basis. While the fixed networks have their area of operation clearly demarcated, with the connectivity maintained with the terminals so connected permanently, the Ad-hoc networks are randomly connected and the count of terminals so connected / disconnected keeps varying. Hence a thorough understanding of this type of network is essential. In this work, an Ad-Hoc Mobile Network termed as MANET is considered which do not locate in a fixed position infrastructure which is shown in the figure 1, but which is formed by the dynamic connections of the nodes. The special feature of these networks is being devoid of any central administrator to monitor / control the communication flow. Hence in such a network, two or many devices or nodes communicate in wireless mode with one another, even without the presence of a centralized administrator.

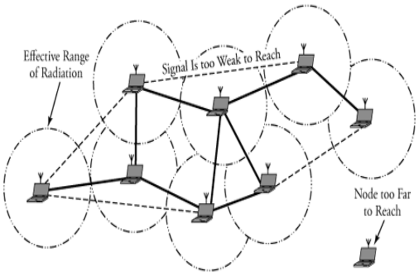

Fig 1: MANET

Each mobile unit becomes responsible as a Host / Router or both and form a part of MANET and deploying it is easy. The features of a general MANET Network are:

a) Nodes are "Self-Organizing".
b) No infrastructure is required.
c) Nodes act as Sender and a receiver.
d) Transmits data simultaneously to multiple receivers

The above reasons ensure MANETS find diverse applications in areas such as Field of war, Rescue operations in times of Natural disasters / calamities such as Floods, earthquakes, Tsunamis, and human induced disasters like industrial accidents.

The working group for MANET standardized routing protocols, was subdivided into routes on- demand or reactive and routes ready-to-use or proactive routing protocols. [2]
In MANETs, the dynamic topology creates additional issues for resolution as each node should be capable to forward data to the other nodes which results in unpredictable connectivity. In the broadcasting mode, a single transmission will lead to multiple receptions. Such transmission protocol when used as a backup enhances the robustness significantly. These protocols use batching which tends to delay the packets. The identification or the intensions of the Mobile devices are neither verifiable nor predetermined. Hence, to maintain the integrity of the nodes, cooperation is essential in receiving and forwarding the request indicates the success in receiving and forwarding the packet. Some nodes may often become incapable of forwarding packets, as they want the resources to be conserved. Few factors like node mobility , scarce resources and limited processing power makes the action of secure communication in wireless networks difficult. In the absence of infrastructure of MANETs which remains unfixed; completely the nodes remain without any constraint, free to move. They act as both host as well as routers for transfer of data packets.

Manuscript published on 30 April 2019.
***** Correspondence Author (s)

K.Madhuri, Computer Science and Engineering,Neil Gogte Institute of Technology, Hyderabad, India.
N Kasiviswanath, Computer science and Engineering, GPREC,Kurnool, Andhra Pradesh, India.

They employ a technique of data transfer to various receivers at the same time , known as multicasting which raises security issues [3] like worm hole outbreaks, black hole outbreaks, Sybil attacks ,Grey hole attacks and neighbor outbreaks as the data is transmitted simultaneously to multiple receivers.

MANET nodes are also called as the routers and are free to move to form a randomly independent system. In ad hoc networks for communication when required to be done between the nodes which are not within their diffusion range, they go for route request and route reply messages. On account of the repetitively as well as firm altering route, the aforementioned remains challenging for maintaining deterministic track. Inherently, the MANETS are prone to attacks of different kinds, as there is no centralized command and control coupled with dynamic topology. Hence security is the main issue in these ad hoc networks. An attack on the communication is basically a third party trying to get hold of the data communication. Different kinds of attacks such as eaves dropping, fake advertisements, packet dropping etc. have been identified. These create problems, of dynamic topology leading to unpredictable connectivity changes as in single packet transmission causing multiple receptions. Using such a transmission system as backup, diminishes the sturdiness of the direction-finding practice considerably.

II. LITERATURE REVIEW

In this effort [7], In [4] writer anticipated a scheme grounded on path termination, path accumulation as well as curved voyage interval, here exist 3 stages on which anticipated procedure mechanisms in leading stage, generate a multi-route for authenticating RREQ, Subsequent stage remains utilized for aggregating that support to recognize entire conceivable routes of the cause as well as endpoint. Here exists computation of usual period of entire paths built on the quantity of expectations in preceding stage.

Towards mitigating wormhole outbreak, in [5] author deliberated a harmless AODV standard direction-finding pattern that is stated by means of TSMI that support, mainly the aforementioned executes on package distribution proportion as well as fragmented relations and moreover interval grounded result alike RTT (round trip time).

In[6] writer anticipated a procedure that is similarly grounded on RTT (Round Trip Time) along with topological evaluation, grouping of both remains discussed by means of RTT-TC. These alterations remain accomplished in AODV direction-finding in MANET. Towards excluding unaffected neighbours commencing the record of distrusted nodules, the deliberated outcome primarily depend on Round Trip Time (RTT) that supports towards identifying distrusted nodes in addition afterwards the Topological assessment.

In [7], writer anticipated a CTPKM using no fundamental conviction individual by the objective of maximizing performance, simultaneously equally qualifying safety accountability. Every single node offers a conviction inception for determining whether or else not to believe additional node. Every node's select formation by means of the well-known conviction inception upsets performance as well as safety of CTPKM. On the base of this limitation customary, the conviction stage, writer takes 3 dissimilar limitations i.e., proficiency, reliability, as well as communal connection.

Writer anticipated a hope centred system grounded on the certification as well as discretion of packages in both direction-finding as well as linkage level, at this time writer utilized conviction assessment consistent with that conviction assessment could crisscross that the designated node remains mischievous or else not in[8].

In [9], writer anticipated a method named PAWAODV (Power-Aware AODV), these methods support towards enhancing the presentation of scheme that consumes inadequate control possessions and by assistance PAW-AODV strategies may accomplish superior by comparing with the standard AODV, Hop-Count limitation is similarly an aspect that supports towards choosing the effective path.

III. PROPOSED SYSTEM

3.1 Wormhole Attack

The attacker receives a packet from node "A" which is tunneled to a point "B" and then broadcasted from that point "B" into the whole network. This causes disruption to the routing. The path from "A" to "B" is called the wormhole link which is essentially a private high speed network. The ease, at which the wormhole attack is played in the network, poses a great risk to the network and is a challenge to defend against it.

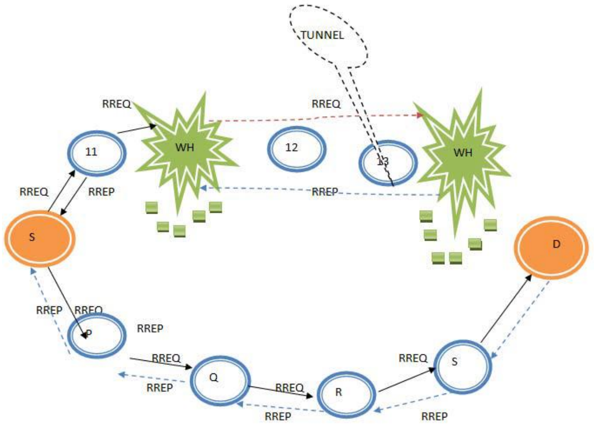

Fig 2: Structure of wormhole attack

Twofold mischievous nodes that produce a channel named worm-hole outbreak that means twofold junction collected nodes which remain extreme separately are connected using a channel generating an anxiety that they remain neighbors. Every single of these nodes permit path appeal as well as topology accomplished transmission commencing the system and direct the aforementioned towards the additional conspire node through channel that determinates and then repeat it attentive in the system beginning at hand. Over this additional channel, these nodes remain capable towards advertising that they ensure the straight route over them.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

As soon as this connection is established, the assailants can pick all further by means of multipoint transmits that at that time direct towards an replace of various topology manage messages and data packets through the wormhole tunnel and Worm-hole node drop all the packets, Show on figure 2.

3.2 Trust based mechanism

Grounded on conviction exemplary aimed at mobile Ad-hoc network, Trusted AODV remains a reliable direction-finding procedure. Affording towards the conviction dealings among them, Trusted AODV consumes numerous appropriate structures identical to nodes performing reliable direction-finding performances mostly. A node which executes mischievous deeds would lastly remain identified and repudiated towards the complete system. Structure repetitive remains enhanced at every single direction-finding stage that remains signified in the flow chart in fig 3.

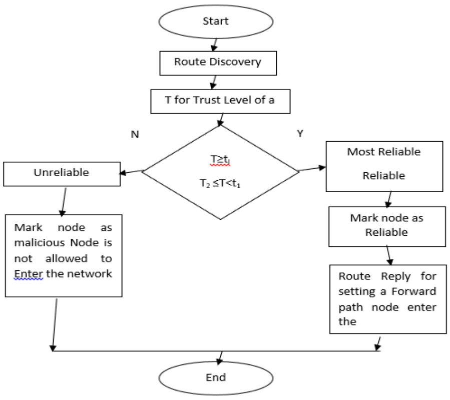
Start
Route Discovery
T for Trust Level of a
N
Y
T≥t1
T2 ≤T<t1
Unreliable
Most Reliable
Reliable
Mark node as malicious Node is not allowed to Enter the network
Mark node as Reliable
Route Reply for setting a Forward path node enter the
End

Fig.3. Flow chart for proposed model

a) Trust category of a node:

The AODV direction-finding procedure remains implanted besides by the **trust function** in this exertion. The transmission among the nodules in the mobile Ad-hoc network is determined by the collaboration and the conviction stage by the aforementioned neighbors. The nodes remain proficient of being categorized hooked on the succeeding grounded on the conviction on neighbor as well as suitable inception standards.

I. **Unreliable:** It is consuming conviction assessment among 0 and 0.5. The non-reliable node remains the defective that means a defective node remains a node through least conviction stage. In the beginning, as soon as some node joints the system, at that time this conviction association by all its neighbors remains small or insignificant that node is preserved as unreliable.

II. **Reliable:** It is consuming trust value between 0.4 and 0.7. These remain the nodes that ensure the conviction stage among the Supreme Trustworthy and Untrustworthy which means a node is reliable to its neighbor and it has received some packets through that node.

III. **Most Reliable:** It is consuming trust value between 0.7 and 1. Most reliable are most trusted nodes or else the nodes with highest trust level may be treated as Most Reliable. Here the higher trust level means neighbors had received or transfer many packets successfully through this particular node.

Each node in cluster computes the conviction assessment aimed at the cluster head. In seeing the twofold mechanisms of conviction i.e. communal conviction as well as QoS conviction, the conviction assessment may be deliberated. Communal conviction comprises the limitations like familiarity, morality, secrecy etc. while QoS conviction comprises limitations like helpfulness, trustworthiness, energy consumption, mission accomplishment etc. We must have utilized energy intake and mission accomplishment as the parameters for calculating the conviction assessment in our anticipated system. The recognition appliance remains as follows:

Towards calculating the conviction assessment aimed at the cluster head remains the main charge in the recognition appliance. Consequently each node in cluster would compute the conviction assessment aimed at the cluster head of the aforementioned group. For calculating the conviction assessment, each node would monitor the behavior of the cluster head. We calculate the trust value by the information composed through controlling the performance of the node. The conviction assessment calculated through every single node remains liberated of each other i.e., conviction assessment deliberated using definite nodes in cluster would not impact the conviction assessment deliberated using additional node in identical cluster. Cluster stage conviction assessment remains intended aimed at the succeeding twofold explanations. One is to ensure the combined outlook regarding the presentation of cluster head as well as further is to consume this conviction assessment by means of the standby aimed at the node stage conviction assessment i.e., if the outbreak drives unnoticed then the aforementioned could remain identified at cluster level, which is shown in the fig.4.

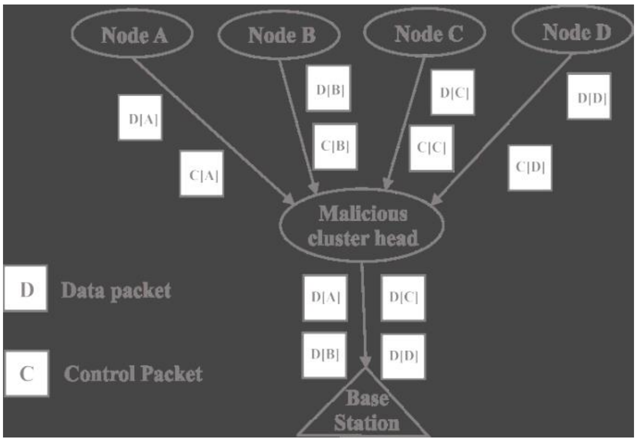

Fig 4: Cluster Head selection process for Malicious

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

IV. RESULT AND DISCUSSION

Table1 shows simulation parameters and values of our proposed work. These nodes remain indiscriminately placed in the extent 1000 × 1000 region in the field of radio range as 250 m. we make use of Application traffic here as CBR (Constant Bit Rate). With simulation time is 1000ms, Packet size is 1000 bytes and maximum speed is 30 m/s. Here we use Master-AODV as routing protocol with channel data rate as 30 Mbps.

Table: 1 Simulation environment

Parameter	Value Taken
Application traffic	CBR
Transmission rate	1000 bytes/0.01ms
Radio range	250m
Packet size	1000 bytes
Channel data rate	30 Mbps
Maximum speed	30 m/s
Simulation time	1000 ms
Number of nodes	100
Area	1000x1000
Mobility model	Random waypoint
Routing protocol	Master-AODV
Attack	Wormhole

The presentation of AODV routing Procedure is analyzed using the performance metrics Throughput, Packet delivery ratio PDR, Delay and Packet drop ratio aimed at varying time intervals and varying number of nodes.

Results

Table.2: Throughput in the presence of wormhole and after prevention.

Time(ms)	Throughput (Attack)	Throughput (Prevention)
2	0.605	0.654
4	0.821	0.871
8	1.044	1.114
10	1.246	1.326

From the above table, we can approximate that the Throughput of AODV is more after relating the avoidance technique than during the attack. The throughput increases as the prevention technique improves the performance.

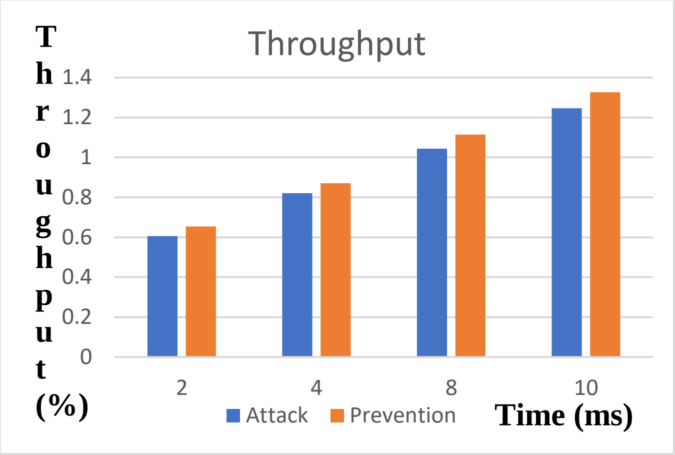

Fig 5: network performance

X-axis: Time Y-axis: Throughput

Throughput is more lately relating the anticipation method, which is shown in the figure 5.

Table 3: PDR in the presence of wormhole and after prevention.

Time(ms)	PDR(Attack)	PDR(Prevention)
2	0.185	0.429
4	0.221	0.562
8	0.517	0.864
10	0.636	0.933

From the above table, we can say that the PDR of AODV is more after applying the prevention technique than during the attack. PDR increases as the prevention technique improves the performance.

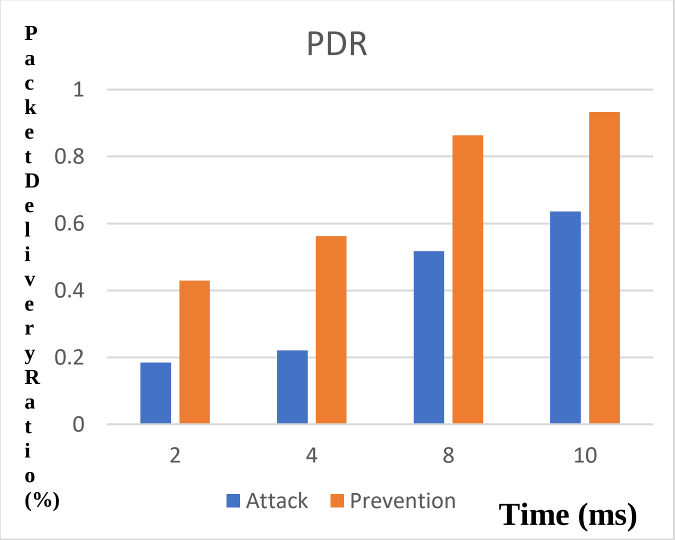

Fig 6: Packet Delivery Ratio

X- axis: Time   Y-axis: PDR

PDR is more after applying the prevention technique, which is shown in the figure 6.

Table 4: Delay in the presence of wormhole and after prevention.

Time(ms)	Delay(Attack)	Delay(Prevention)
2	0.463	0.263
4	1.121	0.921
8	1.676	1.276
10	1.956	1.563

From the above table, we can conclude that the delay ratio is reduced after applying the prevention technique. Packets are delivered more efficiently and the delay ratio is reduced.

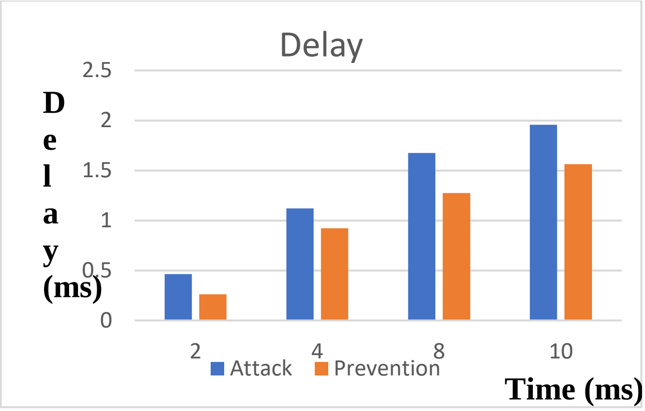

Fig 7: Performance of Delay

X-axis: Time Y-axis: Delay

Delay is less after applying the prevention technique, which is shown in the figure.7.

Table 5 Packet drop ratio in the presence of wormhole and after prevention.

Time (ms)	Packet drop ratio (Attack)	Packet drop ratio (prevention)
2	0.546	0.346
4	0.719	0.519
8	0.976	0.676
10	1.356	0.835

From the above table we can say that the packet drop ratio is reduced after applying the prevention technique. The number of packets dropped is less after applying the prevention technique thus improving the efficiency of MANET.

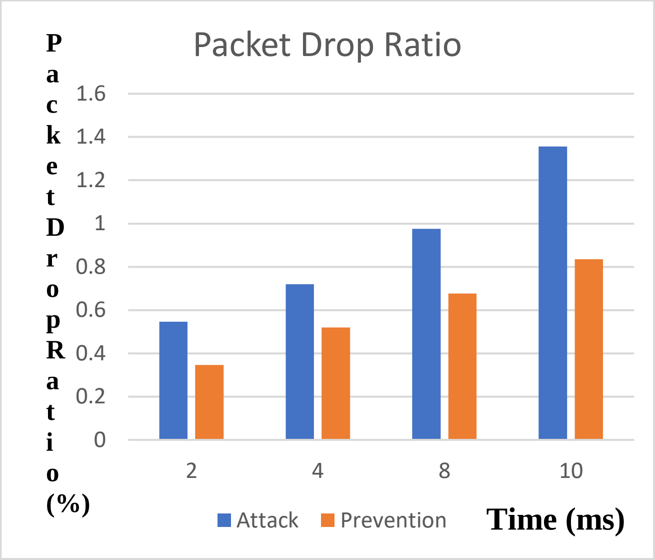

Fig 8: Packet drop ratio

X-axis: Time Y-axis: Packet drop ratio

Packet drop ratio is less after applying the prevention technique, which is shown in the figure 8.

Table 6 Energy Consumption in the presence of wormhole and after prevention.

Time (ms)	Energy Consumption (Attack)	Energy Consumption (prevention)
2	0.435	0.235
4	0.608	0.408
8	0.865	0.565
10	1.245	0.724

From the above table we can say that the Energy Consumption is reduced after applying the prevention technique and thus improving the efficiency of MANET.

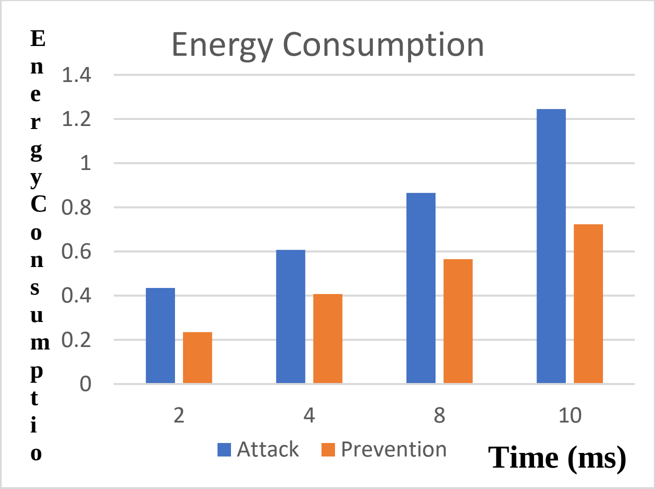

Fig 9: Network Life time

X-axis: Time Y-axis: Energy Consumption

Energy Consumption is less after applying the prevention technique, which is shown in the figure.9.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

V. CONCLUSION

Presence of Wormhole attack in MANET reduces the efficiency of routing in a MANET. After applying the prevention technique based on Trust based mechanism, the performance of the MANET has improved. The performance metrics Throughput and PDR have improved and Packet drop ratio and Delay are reduced. Hence this mechanism has successfully reduced the effect of Wormhole attack in a MANET when AODV routing protocol is used to route the data packets in a MANET and improved the efficiency of MANET routing.

REFERENCES

1. K.Madhuri, Dr.N.KasiViswanath, "Implementation of Position based technique to prevent Worm hole attack in AODV Routing protocol for MANET". International Journal and magazine of Engineering, Technology, Management and Research.Vol 5 2016; pp-11-14.
2. M. Pozza, A. Rao, H. Flinck and S. Tarkoma, "Network-In-a-Box: A Survey About On-Demand Flexible Networks," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2407-2428, thirdquarter 2018. doi: 10.1109/COMST.2018.2807125
3. Gagandeepashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012 269.
4. Soo Young Shin, Eddy Hartono Halim eet al., "Wormhole Attack Detection in MANETs using Route Redundancy and Timebased Hop Calculation", ICT Convergence (ICTC), 2012 International Conference on Jeju Island IEEE,2012. Pages 781 – 786.
5. Isaac Woungang, Sanjay Kumar Dhurandher, Mohammad S. Obaidat, IssaTraore et al.,"Timed And Secured Monitoring Implementation Against Wormhole Attack in AODV-Based Mobile Ad Hoc Networks", IEEE, May 2013 pages 1-5.
6. Mohammad RafiqulAlam, King Sun Chan et al.,"RTT-TC: Topological Comparison Based Method to Detect Wormhole Attacks in MANET", Communication Technology (ICCT), 2010 12th IEEE International Conference on Nanjing IEEE, 2010 pages 991 – 994.
7. Jin-Hee Cho, Kevin S. Chan, Ing-Ray Chen et al., "Composite Trust-based Public Key Management in Mobile Ad Hoc Networks", ACM 28th Symposium on Applied Computing,2013 Pages 1949-1956.
8. Naveen Kumar Gupta, Kavita Pandey et al., "Trust Based Adhoc On Demand Routing Protocol for MANET", Contemporary Computing (IC3), 2013 Sixth International Conference on Noida IEEE, 2013 pages 225-231.
9. Chee-Wah Tan, Sanjay Kumar Bose,etal.,"Modifying AODV for Efficient Power-Aware Routing in MANETs" , TENCON 2005 2005 IEEE Region 10 Melbourne, Qld IEEE,2011 pages 1-6.