Journal of
Electrical & Electronic Systems

Kaur and Gupta, J Electr Electron Syst 2014, 3:3
DOI: 10.4172/2332-0796.1000133

Research Article Open Access

Intrusion Detection System for Wormholes in WSN

Harleen Kaur[1]* and Neetu Gupta[2]

Department of ECE, GIMET, Amritsar, Punjab, India

Abstract

As an increasing number of people are going wireless, reducing the criticism of wireless networks is becoming a top priority. Wormhole attack is a severe threat against ubiquitous sensor networks. In a wormhole attack, the intruder sniffs the packets at one point in the network and forwards them with a less latency and relays them to another point in the network. A strategic placement of the wormhole can result in a significant breakdown in communication across a wireless network. The objective of dissertation addresses the efficient comparing the proposed technique with the previous study. In this paper, we have proposed an algorithm where intrusion detection has been done in a proposed approach to detect the wormhole attacks. The AODV routing protocol is used as the underlying network topology. Data tracker is used for detecting and isolating the malice node i.e. acting as a wormhole. This approach is implemented by using NS-2. The Simulation results are presented to validate the stated goal by comparing various performance metrics.

Keywords: Wormhole; AODV (Ad-Hoc on Demand Distance Vector Protocol Vector); Wireless network; Intrusion detection system; Routing

Introduction

Intrusion Detection System (IDS) in wireless networks has played an important role in network security by providing an additional level of protection to the network topology and applications beyond the traditional security mechanisms such as encryption and authentication. It detects the attacks and isolates the malicious nodes by matching the patterns of known intrusions or discovering the anomalies in the network activities. Its application environments cover almost all wireless networking scenarios such as ad hoc networks, wireless LANs, and sensor network [1]. Wireless Sensor Networks (WSNs) have been applied in more and more applications; however in sensor network sensor nodes are responsible not only for-the monitoring of the environment but also for forwarding the data packets toward base station on behalf of other sensor nodes. The sensors must be able to trace the routes to the base station and aware of their neighbours. An attacker can easily access of this, and may try to control the routes and to monitor the data packets that are sent along these routes [2]. One way to achieve this is to set up a wormhole in the network. A wormhole is a specialized man in- the-middle attack in which the adversary connects two otherwise distant regions of the network. We proposed a scheme for intrusion detection in WSN. They proposed distributed and cooperative framework to detect the attack. Every node in the WSN participates in the process of intrusion detection. It detects the sign of intrusion locally and independently and also propagates this information to other nodes in the network. Intrusion Detection is a security technology that attempts to identify individuals who are trying to break into and misuse a system without authorization and those who have legitimate access to the system and are abusing their privileges. The system protected is used to denote an information system being monitored by the Intrusion Detection system. Routing protocols [3] like table-driven/proactive, demand-driven/reactive or hybrid variants are subjected to routing attacks resulting in compromised confidentiality, integrity and message authentication.

Outline of the paper

The rest of this paper is organized as follows. A brief survey of related work is given in the next section. Section II describes the wormhole attack model and its types for implementing the wormhole attack. Section III shows the related work and its solution. In Section IV proposed algorithm for detection and isolation method is described. In Section V an analysis of the results is presented. Finally conclude the paper in section VI.

Wormhole Attack

In the wormhole attack, an attacker tunnels messages received in one part of the network over a low latency link and replays them in a different part. The simplest instance of this attack was a single node situated between two other nodes forwarding messages between the two of them as shown in Figure 1. However, wormhole attacks more commonly involve two distant malice nodes colluding to understate their distance from each other by relaying packets along an out-of-

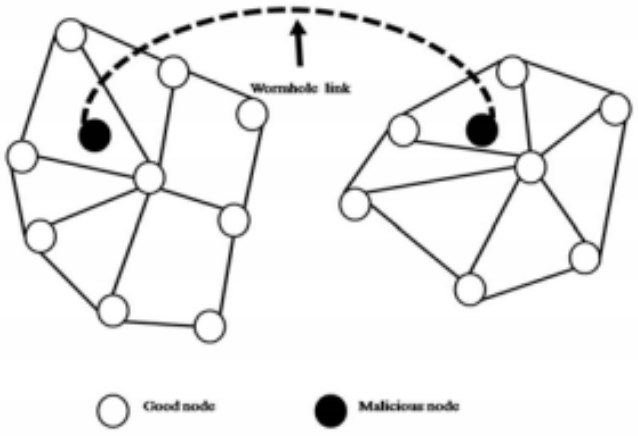

Figure 1: Wormhole attack.

***Corresponding author:** Harleen Kaur, Department of ECE, GIMET, Amritsar, Punjab, India, E-mail: harleen.kaur15@yahoo.com

Received September 15, 2014; **Accepted** September 26, 2014; **Published** October 07, 2014

Citation: Kaur H, Gupta N (2014) Intrusion Detection System for Wormholes in WSN. J Electr Electron Syst 3: 133. doi:10.4172/2332-0796.1000133

bound channel available only to the attacker. An attacker is situated close to a base station can easily disrupt routing by creating a well-placed wormhole and convince the nodes that they were only one or two hops away via the wormhole. This can create a sinkhole: that is the attacker on the other side of the wormhole draws all the traffic if alternate routes are less attractive and provides artificially a high-quality route to the base station. This will most likely always be the case when the endpoint of the wormhole was relatively far from a base station [4].

Types of wormhole attack

Wormhole attacks are divided on the basis of implementation technique used for launching it and the number of nodes involved in establishing wormhole into the following types:

Encapsulation of the packet: Wormhole attacks are the disaster against many ad-hoc routing protocols, such as the two ad-hoc on-demands routing protocols DSR and AODV, and the sensor Tiny OS beaconing routing protocol. In DSR, RREQ floods the traffic in the network, when node S needs to discover a route to a destination, say D. Any node that receives the request, adds its identity to the source route, and rebroadcasts it. Each node broadcasts only the first route request it receives and drops any further copies of the same request. D generates a route reply when it receives each route request and sends it back to S and selects with the shortest number of hops or the path associated with the first arrived reply. This protocol will fail in a malice environment. When a malicious node at one part of the network receives the route request packet, it send to a second colluding party at a distant location near the destination, then the two colluding nodes will be said to have a wormhole . This prevents nodes from discovering true paths that are more than two hops away.

Consider Figure 2 in which nodes A and B try to maintain the shortest path between two spiteful nodes X and Y. Node A broadcasts a route request (RREQ), X gets the REQ and encapsulates it in a packet destined to Y through the path that exists between X and Y (U-V-W-Z). Node Y de marshals' the packet, and replays it again, which reaches B. The hop count does not increase during the traversal through U-VW-Z due to packet encapsulation. From A to B request travels through C-D-E. There are two routes for node B, the first is four hops long (A-C-D-E-B), and the second is apparently three hops long (A-X-Y-B). Node B will choose the second route since it appears to be the shortest while in reality it is seven hops long. So X and Y succeed in involving themselves in the route between A and B. A simple way of countering this mode of attack is a by-product of the secure routing protocol ARAN, which chooses the fastest route reply rather than the one which claims the shortest number of hops.

Out-of-band channel: In this mode, the wormhole attack was

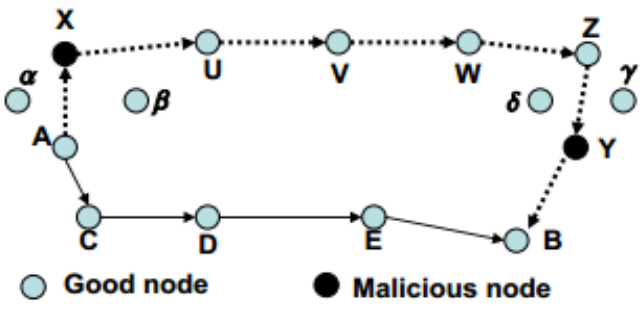

Figure 2: Packet Encapsulation.

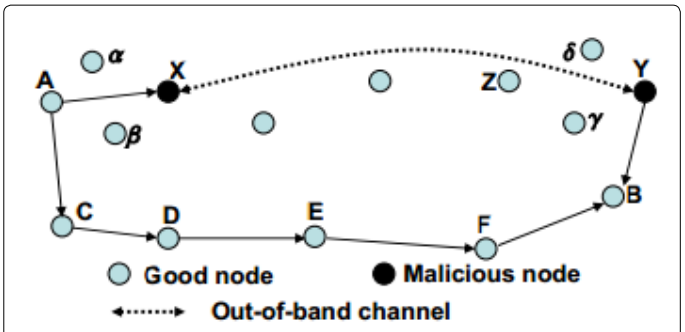

Figure 3: Out of band channel.

launched by having a high-quality, single-hop, out-of-band link (called tunnel) between the malicious nodes. By using a long-range directional wireless link this tunnel is achieved. This mode of attack was more difficult to launch than the packet encapsulation method since it needs specialized hardware capability [5].

Consider the scenario depicted in Figure 3. Node A is sending a route request to node B, nodes X and Y are malicious having an out-of-band channel. Node X tunnels the route request to Y, which is a true neighbour of B and node Y broadcasts the packet to its neighbours. Node B gets two route requests-A-X-Y-B and A C-D-E-F-B. Node B chooses the first route which is shorter and faster than the second and thus wormhole is established between X and Y in the route between A and B.

High-power transmission capability: In this type of wormhole attack, only one malice node with high-power transmission can communicate with other normal nodes from a long distance. When a malice node receives an RREQ, it broadcasts the request at a high-power level and rebroadcasts the RREQ towards the destination so that another node hears. By this method, the spiteful node increases its chance to be in the routes established between the source and the destination even without the participation of another malicious node. This attack can be minimized if each sensor node measures the received signal strength accurately [4].

Packet relay: Packet-relay-based wormhole attacks can be launched by one or more malicious nodes. In this attack, a malice node relays data packets of two distant sensor nodes to convince them that they were neighbour. This kind of attack was also known as "replay-based attack".

Protocol distortion: In this mode of wormhole attack, one malicious node tries to sniffs the network traffic by distorting the routing protocol. Routing protocols that were based on the 'shortest delay' instead of the 'smallest hop count' was at the risk of wormhole attacks and also called as "rushing attack".

Related Work

Detection of wormhole attack has been an active area of research and many mechanisms have been proposed so far luring the various behaviours of wormhole attack.

Kashyap Patel and Manoranjitham [6] addresses several types of sensor nodes and many network layer attacks can be perform on the network. Wormhole Attack was one of them which were most destructive routing attack for wireless sensor network and can be implemented by using Mint route protocol. In wormhole attack two or more node creates a Virtual tunnel in that network which transfer data

packet. This virtual tunnel creates the shorter link in wireless sensor network. This paper presents the high level security and detection of wormhole attack by using Simulation results.

Issa Khalil et al. [7] represent the multihop wireless systems to relay each other's packets expose them to a wide range of security attacks. A particularly severe threat was known as the wormhole attack, where spiteful nodes records and control the data traffic at one location and tunnels it to another node, which replays it locally. For such sensor networks. A lightweight countermeasure for the wormhole attack, called LITEWORP was suitable for resource-constrained. Simulation results show that every wormhole was detected and isolated within a very short period of time. The results also show that the fraction of packets lost is less when LITEWORP was applied.

Yih-Chun Hu et al. [8] represents wormhole attack, a severe attack in the network that was particularly challenging to defend against and was possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. The wormhole attack can form a serious threat in wireless networks, against many network routing protocols and location-based wireless security systems. A general mechanism, called packet leashes, for detecting and defending against wormhole attacks, and a specific protocol, called TIK that implements leashes. Topology-based wormhole detection was discussed, and shows that it was impossible for these approaches to detect some wormhole topologies.

Bintu Kadhiwala and Harsh Shah [9] propose the security emerges as a central requirement as mobile ad hoc network applications were deployed. Wormhole attacks enable an attacker with limited resources and no cryptographic material to wreak havoc on wireless networks. It is possible even if the attacker has not compromised any hosts and all communication provides authenticity and confidently. Wormhole attacks can form a serious threat in wireless networks.

Devendra Singh et al. [10] addresses the multiple –hop Mobile ad hoc networks which establish the routes involving with each node acting as a host and router. The wormhole attack was considered to be a serious security attack in multi-hop ad hoc networks. A simple technique to effectively detect wormhole attacks without the need for special hardware and/or strict location or synchronization requirements was proposed. The base of dissertation is to find alternative path from source to second hop and calculate the number of hops to detect the wormhole.

Saurabh Gupta et al. [11] represent specific attack called Wormhole attack that enables an attacker to record packets at one location in the network, send them to another location, and retransmits them into the network. After the route discovery, source node initiates wormhole detection process in the established path which count shop difference between the neighbours of the one hop away nodes in the route. If the hop difference between neighbours of the nodes exceeds the acceptable level then the destination node detects the wormhole. Our simulation results show that the WHOP is quite excellent in detecting wormhole of large tunnel lengths.

Proposed Work

Brief overview of proposed algorithm

- Divide the network in number of zones information of number of nodes and packet routing.
- Select the leader for the respective zones giving the information of each node.
- Assign the data tracker for each zone keeping the track of data send and received by the destination.
- Mismatch between data sent by source and received by destination will lead to the detection of the wormhole in the network.
- If the number of received packet - number of forwarded packets was more.
- Isolate the wormhole nodes from the network by sending alert messages to the nodes.
- Nodes after receiving the alert message will not communicate with the wormhole.

Network consists of number of nodes. To start the simulation, wormhole attack is created with animated rate of 5 ms and movement of the nodes are started at 0.1 sec in the network. At 2.0 sec all the mobile nodes are placed in the area of 40 m. Now divide the network into number of clusters. Each cluster has its own leader i.e. its own cluster head. The cluster head is elected on the basis of energy the node having the highest energy is elected as the leader. To each cluster data tracker is assigned. Data tracker contain all the information about the number of nodes in the cluster, number of packets forwarded and receive and communication path. When CBR is attached with UDP, communication between the nodes is started. After 14 sec tunnel is created between the two nodes i.e. wormhole is present. Wormhole is detected if threshold value (number of forwarded packets – number of received packets) is more and to isolate the scheme two nodes are created in the path through which data packets are send i.e.by sending the alert message to the nodes. Nodes after receiving the alert message will not communicate with the wormhole

Simulation Results

The results are shown below deals with the comparison of the routing protocol with mobile nodes. The work focuses on traceability of the wormhole attack. The result of this work is derived by using NS2 simulator.

NS-2 was used to verify the performance of the previous and proposed wormhole mechanisms. The network topology illustrates that there were fifty six random movable regular nodes with maximum speed in 5m/s randomly distributed in an area of 1100 m×1100 m, and AODV was performed for regular routing. A pair of wormhole nodes is developed wherein two tunnel nodes were applied to play the secret tunnel for wormhole attack. A connection with UDP-CBR is set up for communication (Figures 4-7).

The above results show the comparison between AODV and DSDV for the wormhole attack on the basis of performance metrics. As the results of DSDV are based on the routing table and number of hop counts and in AODV routing protocol, routes are established dynamically at intermediate nodes. Each node maintains sequence numbers to determine freshness of routing information and avoid routing loops. The impact of the above mentioned results for AODV will check out Wormhole attack when cluster head does not receive any data from the mobile nodes. The data tracker informs all the nodes and cluster head to trace the wormhole attack. The proposed AODV and base DSDV routing protocol produce result for tracing and isolation of wormhole attack by calculating its throughput and overhead. From the Figure 7 of throughput it shows that throughput of AODV routing protocol is more as compared with routing protocol DSDV. From the

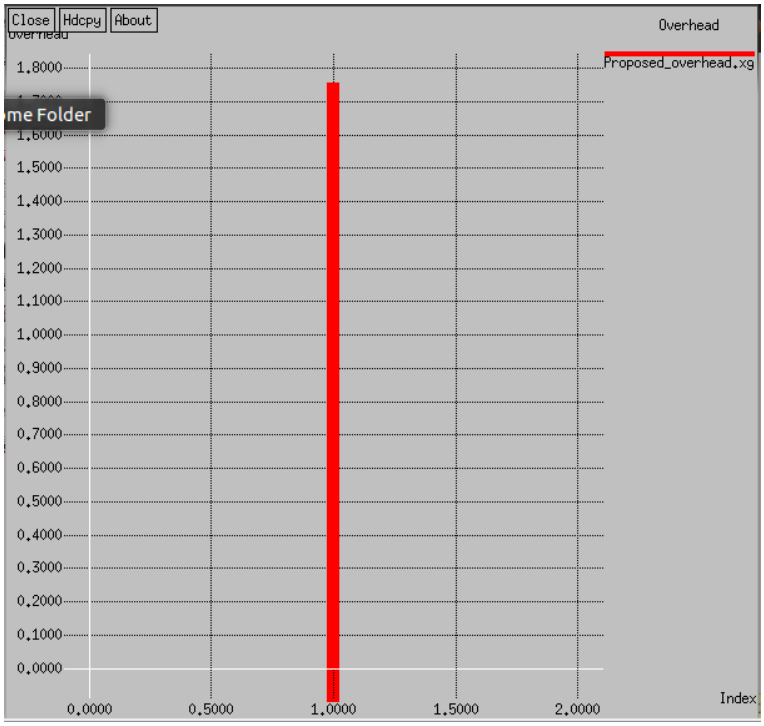

Figure 4: Proposed Overhead.

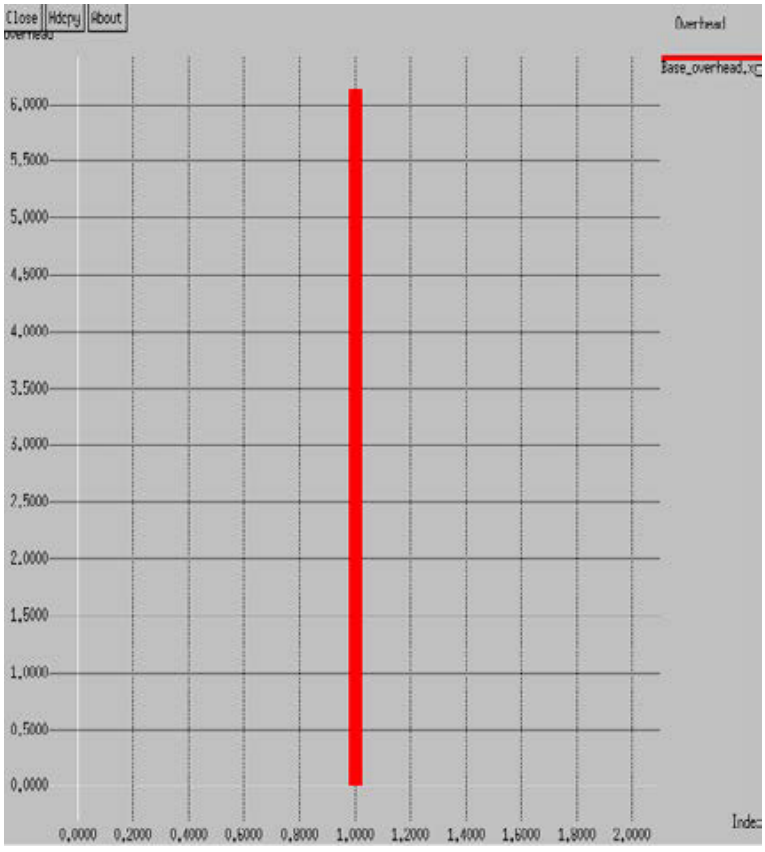

Figure 5: Base Overhead.

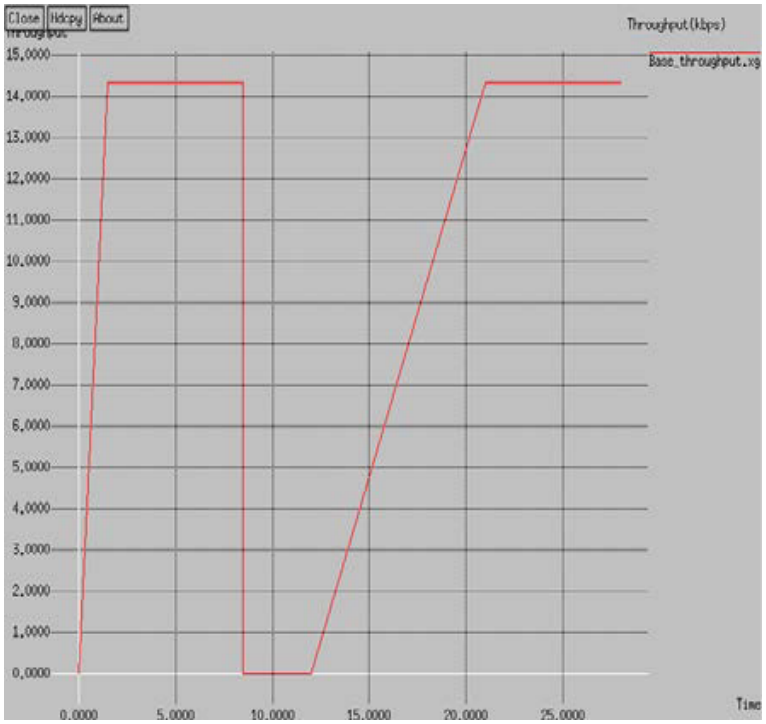

Figure 6: Base Throughput.

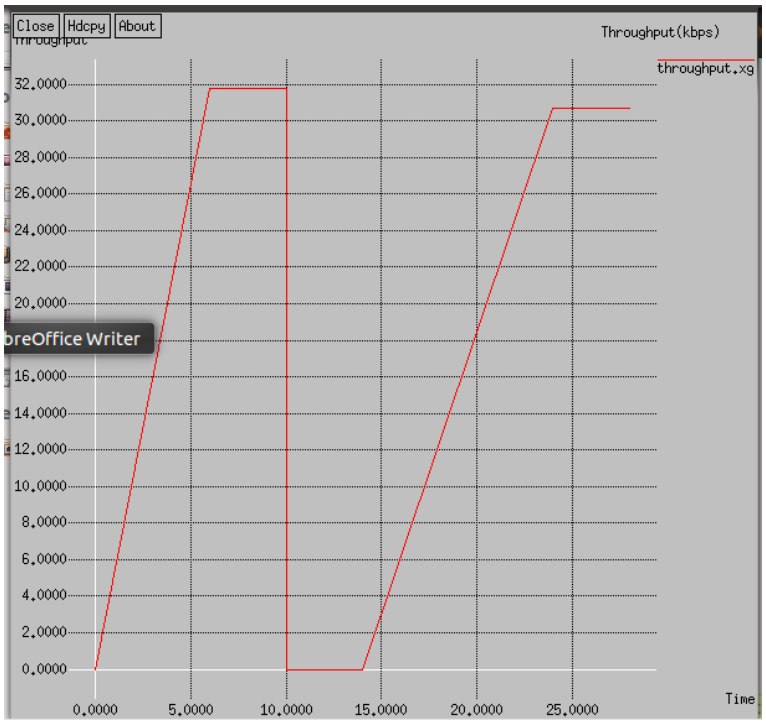

Figure 7: Proposed Throughput.

Figure 4, it shows that overhead of AODV is less as compared with DSDV i.e. overhead of 1.75 is observed which signifies the amount of routing required to transmit the data in the network is 1.75 times the data packets in AODV.

Conclusion and Future Work

The deployment of mobile nodes in an attended environment makes the network vulnerable. This paper gives a bird eye over WSN and intrusion of malicious nodes may cause serious impairment to security.

Wormhole presents an illusion of shortest path and tries to attack all the traffic over the network. The objectives listed have been carried out. In the presented work, we have discussed the routing protocol AODV with their working. With the results of AWK programming and trace graph, we can conclude that in the case of simple AODV increases in throughput by isolating the wormholes and decrease in the packet overhead by 1.75 and in future, work out with the unprotected protocols different types of attacks including group attacks and their relations can be studied and to study the robustness of Wireless Ad Hoc Networks for all types of protocols.

References

1. Wang W, Lu A (2006) Interactive Wormhole Detection in Large Scale Wireless Networks, IEEE Symposium on Visual Analytics Science and Technology, Baltimore, MD, USA.
2. Butty´an L, D´ora L, Vajda I (2005) Statistical Wormhole Detection in Sensor Networks. Lecture Notes in Computer Science Springer-Verlag Berlin Heidelberg ESAS 3813: 128-141.
3. Stephen Glass NICTA, Vallipuram Muthukkumurasamy, Marius Portmann (2013) MLDW- a Multilayered Detection mechanism for Wormhole attack in AODV based MANET, International Journal of Security, Privacy and Trust Management.
4. Sharma N, Singh U (2014) Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks. International Journal of Computer Science and Mobile Computing 3: 29-33.
5. Issa Khalil (2007) Mitigation of control and data traffic attacks in wireless Ad-hoc and sensor networks, Purdue University.
6. Patel K, Manoranjitham T (2013) Detection of wormhole attack in wireless sensor network, International Journal of Engineering Research & Technology (IJERT).
7. Khalil I, Bagchi S, Shroff NB (2005) LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks, Proceedings of the 2005 International Conference on Dependable Systems and Networks.
8. Hu Y-C, Perrig A, Johnson DB (2006) Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communications 24: 370-380.
9. Kadhiwala B, Shah H (2012) Exploration of Wormhole Attack with its Detection and Prevention Techniques in Wireless Ad-hoc Networks, International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS-2012).
10. Singh D, Khare KA, Rana JL (2013) Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET. International Journal of Computer Applications (0975-8887) 62: 21-25.
11. Gupta S, Kar S, Dharmaraja S (2011) WHOP: Wormhole Attack Detection Protocol using Hound Packet, IEEE International Conference on Innovations in Information Technology.