Paper Title (TIJER SAMPLE PAPER (24pt, Times New Roman, lower case, line spacing: Before: 8pt, after: 16pt)

1st Author, 2nd Author,3 3rd Author

1Designation of 1st Author,2Designation of 2nd Author,3Designation of 3rd Author

1Name of Department of 1st Author,

1Nameoforganization of 1st Author, City,Country

1Author1@xyz.com, 2Author2@xyz.com, 3Author3@xyz.com

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Abstract** - Cognitive radio is widely expected to be the next Big Bang in wireless communications. Spectrum sensing, that is, detecting the presence of the primary users in a licensed spectrum, is a fundamental problem for cognitive radio. In this paper spectrum sensing techniques are reviewed.

**Index Terms** - Component Cognitive Radio (CR), Dynamic Spectrum Access (DSA), Primary User (PU), Secondary User (SU), Software Defined Radio (SDR)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **Introduction (Heading 1)**

Polyvinyl chloride, more commonly known as PVC, is a building block of various products, such as electronic items, constructional materials, stationeries, chemical equipments, wires, cables etc. It is one of the major thermoplastics used today and produced in a huge amount worldwide [1, 2]. be improved [1, 2]. Commercially, compounding PVC contains sufficient modifying components to the raw polymer to produce a homogeneous mixture suitable for processing and requiring performance at the lowest possible price. The proper compounding and processing PVC resin using suitable additives produces a complex material whose behavior and properties are quite different from the PVC resin by itself [10]. The selection of particular additive is dependent on the end use of the PVC product like PVC-resin is not plasticized for the use in making rigid products such as water pipe, plumbing fittings, and phonograph records.



**Fig.1 Screw prepared by lathe machine by using of mould**

****

# **Literature survey**

**Vikash Agarwal, Jyoti Vimal. et al [11**] have been found out optimization of extrusion blow molding process parameters by grey relational analysis and Taguchi method. This research work based on extrusion blow molding process for making plastic container of high density polyethylene grade B6401 (HDPE) and experimental runs based on an L9 orthogonal array of Taguchi method. The Taguchi method was performed on plastic material and the process parameters were blowing temperature, blowing time and exhaust/cooling time.

**Crane Girder Design [4]**

**Find cross section of gantry girder**

Z = $\frac{M}{σ}$ = $\frac{1806×10^{6}}{0.66 ×250}$ = 11 × 106  mm3

The section modulus increased by 25 percent to actual for bending

Zreq = 1.25 × 11 × 106  mm3  = 13.75 × 106  mm3

Here select box section for girder [5] as shown in figure.



**DRUM DESIGN**

Dimension of drum and pulley are depending on the wire rope diameter.

Diameter of drum measured at the bottom of the groove shall not be less than the value calculated by using following formula:

Dd = 12 ×d ×Cdf ×Crc [3]

D = 32 mm Cdf  = 1.5 Crc = 1.25

Standard Diameter of drum at the bottom the groove from IS 3177:1999 [3] is 800 mm.

Radius of Groove shall be 17.60 in mm as shown in figure 10.

****

 Figure 3-D model of drum Figure .Fixed support and load application

# **WORMHOLE ATTACK TAXONOMY**

Wormhole attack can be achieved with the help of several techniques such as packet encapsulation, high transmission power and high quality communication links etc.

(1)Wormhole Using Encapsulation

Several nodes exist between two malicious nodes and the data packets are encapsulated between the malicious nodes. Encapsulated data packets are sent between the malicious nodes, so the actual hop count does not increase during the traversal. Routing protocols that use hop count for path selection are particularly susceptible to encapsulation-based wormhole attacks. For example, AODV (Ad hoc On Demand Routing Protocol) fails under encapsulation based wormhole attacks. When a malicious node at one part of the network hears the route request message (RREQ), it transmits this RREQ to the other malicious node at a distant location near the destination. The second malicious node then rebroadcasts the RREQ. The neighbors of the second malicious node then receive the RREQ and drop any further legitimate RREQs that are coming from legitimate multi-hop paths. As a result, the route between the source and the destination include the malicious nodes that form the wormhole. This prevents the sensor nodes from discovering legitimate paths that are more than two hops away.

(2)Wormhole Using High Quality Channel

The wormhole attack is launched by having a high quality, single hop, out -of-band link (tunnel) between the malicious nodes. This tunnel can be achieved by using a direct wired link or a long range directional wireless link. This mode of attack is more difficult to launch than the packet encapsulation method since it needs specialized hardware capability.

(3)Wormhole Using High Power Transmission Capability

Only one malicious node with high power transmission capability exists in the network and this node can communicate with other normal nodes from along distance. When a malicious node receives a RREQ, it broadcasts the request at a high power level. Any nodes that hear the high power broadcast rebroadcasts the RREQ towards the destination.



Fig.3 Wormhole Attack

# **conclusions**

Wormhole attack in wireless sensor network can disturb the routing process and ultimately degrade network performance. In this paper, we have presented existing wormhole attack types and their detection mechanism. Wormhole detection in a dynamic WSN setting is an open research area. A good research direction for wormhole detection is integration of trust based systems and time or distance bounding wormhole detection techniques.

# **references**

**[**1] Thanassis Giannetsos, Tassos Dimitriou, Neeli R. Prasad “State of the Art on Defenses against Wormhole Attacks in Wireless Sensor Networks” *Wireless VITAE 2009: 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory& Electronic Systems Technology*, pp. 313- 318.

[2] I. Krontiris, T. Giannetsos, and T. Dimitriou, “Lidea: A distributed lightweight intrusion detection architecture for sensor networks,” in *SECURECOMM ’08: Fourth International Conference on Security and Privacy for Communication Networks*, Istanbul, Turkey.

[3] Y. C. Hu, A. Perrig, and D. B. Johnson, “Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks,” in *Proc. Of IEEEINFOCOM*, 2003, pp. 1976-1986, vol 3

[4] L. X. Hu and D. Evans, “Using directional antennas to prevent wormhole attacks,” in *Proc. IEEE Symp. Network and Distributed System, Security (NDSS 04*), San Diego; February 2004.

[5] Bayrem TRIKI, Slim REKHIS, and Noureddine BOUDRIGA “Digital Investigation of Wormhole Attacks in Wireless Sensor Networks” *Eighth IEEE International Symposium on Network Computing and Applications,* 2009, pp. 179-186.

[6] Zhibin Zhao; Bo Wei; Xiaomei Dong; Lan Yao; Fuxiang Gao; **“**Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis” *International Conference on Information Engineering(ICIE),* 2010, pp. 251-254.

[7] Prasannajit B, Venkatesh, Anupama S, Vindhykumari K, Subhashini S R, Vinitha G; “An approach towards Detection of Wormhole Attack in Sensor Networks”*First International Conference on Integrated Intelligent Computing (ICIIC)*, 2010, pp. 283 – 289.

[8] W. Wang and B. Bhargava, “Visualization of wormholes in sensor networks” *WiSe’04,* *Proceeding of the 2004 ACM workshop on Wireless Security* , ACM Press, pp. 51-60, 2004.

[9] S. Ozdemir, M. Meghdadi and I. Guler, “A time and trust based wormhole detection algorithm for wireless sensor networks” in 3rd Information Security and Cryptology Conference (ISC’08), pp. 139-142.