ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 7, July 2017

SECURE ROUTING IN WIRELESS SENSOR NETWORK

Ms. Sweety Gupta

Abstract

Remote Sensor Networks are thickly conveyed ease, low handling power, less memory and constrained vitality asset systems. As of late WSN found an expansive number of utilizations in the field of both research and scholastics. In WSN, the hubs are called sensors which sense the information like temperature, mugginess, clamor or sound, weight soil assortment, developments of items, stretch levels, recognition of articles around and different properties from the encompassing and send this data to the base station for assist examination and basic leadership. WSN are primarily conveyed in indigenous habitat where the sensor hubs stay unattended and utilized for observation and checking.

I.Introduction

WSN unearths a huge utility in the fields like military, site visitors manipulate, home automation, healthcare applications and lots of civilian software regions. Since WSN sensor nodes are deployed in unattended and difficult natural surroundings there are large wide variety of protection issues with them. Data transmitted in WSN should be safeguarded from unauthenticated and unauthorized nodes and attackers. We should preserve the authenticity, integrity and confidentiality of the data that is transmitted between the nodes of the network. Intruder may additionally attack the community in lots of approaches as tampering and jamming the information packets affect the integrity, unauthorized get right of entry to to the network, pretending to be authenticated node to capture the facts. There are many routing protocols for keeping and management of WSN. Different categories of routing protocols are flat-based, Hierarchical, location-based, Network float and QoS, Mobility-based, Multipath-based totally, Heterogeneity-primarily based protocols. The above mentioned class deals with maintenances and management routing information, making the network to stay longer by means of lowering the electricity intake (power efficient) and keep community infrastructure. All the protocols lacks in imparting right security mechanism for Wireless Sensor network. There is not any right layered fashionable for Wireless Sensor Networks. Here is a summarized view of viable assaults and their safety answers.

II. SECURITY REQUIREMENT

A sensor network is a special type of ad hoc network. Sensor network is quiet similar to ad hoc networks .The security requirement [1] of a wireless sensor network can be defined in following ways:

- **Authentication:** As WSN communicates sensed data that is going to help us in making important decision. The receiver needs to ensure that the data used in any decision making process originates from the correct source. Similarly authentication is necessary during exchange of control information in the network.

- **Integrity:** Data in transit can be changed by the attacker. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Data integrity is to ensure that information is not changed in transit either due to malicious intent or by accident.
- **Data Confidentiality:** Application like surveillance of information, industrial secrets and key distribution need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption.
- **Data Freshness:** Even if confidentiality and integrity are assured, we also need to ensure the freshness of each message. Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To ensure that no old messages replayed a time stamp can be added to the packet.
- **Availability:** Sensor nodes may run out of battery power due to excess computation or communication and become unavailable. It may happen that an attacker may jam communication to make sensors unavailable. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the network.
- **Secure localization:** The sensor network often needs location information accurately and automatically. However an attacker can easily manipulate non-secured location information by reporting false signal strengths and replaying signals, etc.

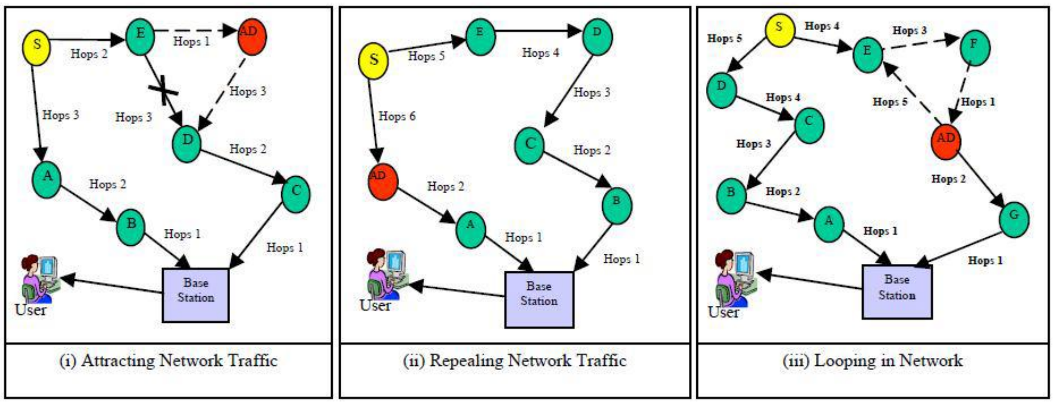
III. ATTACKS IN WSN

Most of the routing protocols proposed for sensor networks and ad hoc network are not designed to handle security related issues. Therefore there is a lot of scope for attacks on them. Different types of attacks on WSN are:

- Spoofed, altered, or replayed routing information
- Selective forwarding attack
- Sinkhole attacks
- Sybil attack
- HELLO flood attack
- Black hole attack

Spoofed, altered, or replayed routing information:

It is the maximum common assault on routing protocols. In this assault the attacker goal the information this is going to be exchanged between the nodes. The attacker may be capable of create routing loop, entice or repel network visitors, enlarge or shorten source routes, generate fake mistakes messages, partition the community, and increases stop to stop delay. The widespread answer for the attack is authentication i.E., routers will best take delivery of routing records from legitimate routers. Figure 1 (i) & (ii) show how attacker can appeal to and repel the network traffic respectively, by means of advertising and marketing a fake path. Figure (iii) offers a situation wherein an attacker node creates a routing loop in the network.



(i) Attracting Network Traffic

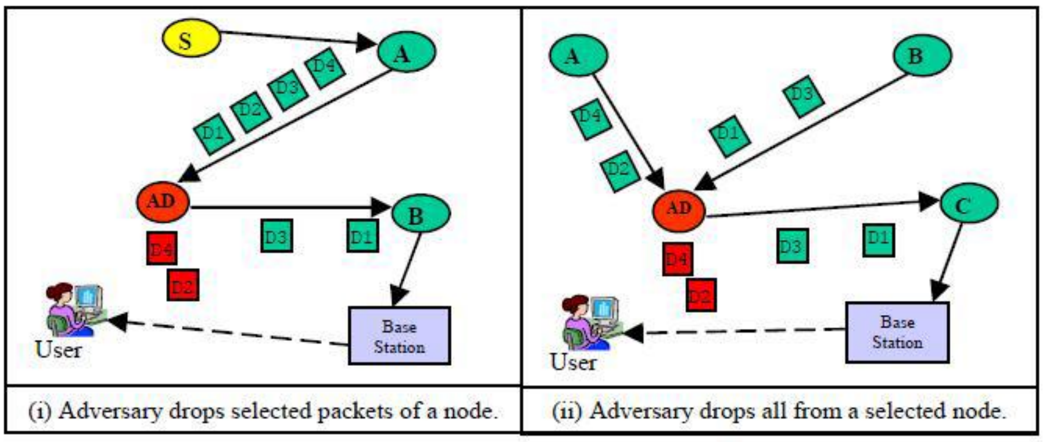
(ii) Repealing Network Traffic

(iii) Looping in Network

Figure 1: Spoofed attack, altered, replayed routing information

Selective forwarding attack:

In wireless sensor community statistics is generally collect in multi hop mode. Multi hop community expect that taking part nodes in faithfully ahead and receive information packets. The attacker might also introduce any malicious node inside the community. This malicious node may refuse to forward records packets and in reality drop them, ensuring that they do not propagate similarly inside the community. The option to this attack is to check the series wide variety properly. Addition of records packet sequence number in packet header can reduce this attack. This assault occurs at community layer inside the wireless sensor network. This kind of attack is viable on hierarchical based totally routing protocols; area primarily based routing protocols, Network waft and QoS conscious protocols. Figure 2(i) and (ii) show scenarios of selective ahead its facts forward assault. In discern (i), source node 'S' forwards its statistics packets D1, D2, D3, D4 to node 'A' and 'A' forward these acquired packets to node 'B'. On other hand an attacker node AD selectively forwards packets D1,D3 even as dropping packet D2 and D4. In another scenario shown in determine (ii) , an attacker may additionally selectively drop packet originated from one supply and forward that of others.



(i) Adversary drops selected packets of a node.

(ii) Adversary drops all from a selected node.

Figure 2: Selective Forward attack

Sinkhole attack:

In the sink hollow attack [1], the attacker attempt to appeal to the almost all of the traffic from a selected area through a compromised node. A compromised node that's positioned at the centre of a few vicinity creates a huge “have an effect on”, attracting all visitors destined for a base station from the sensor nodes. The attacker targets a place to create sinkhole where it could entice the most visitors, probably in the direction of the base station in order that the malicious node can be perceived as a base station. Sinkholes are difficult to defend in protocol that use advertised statistics together with last strength or an estimate of quit to cease reliability to assemble a routing topology because this records is hard to verify. This attack occurs at network layer. This sort of assault is feasible on flat based routing protocol, hierarchical routing protocols, Network float and QoS conscious routing protocols. The determine 3 demonstrates sinkhole attack where ‘SH’ is a sinkhole. The sinkhole attracts visitors from almost all of the nodes to route through it.

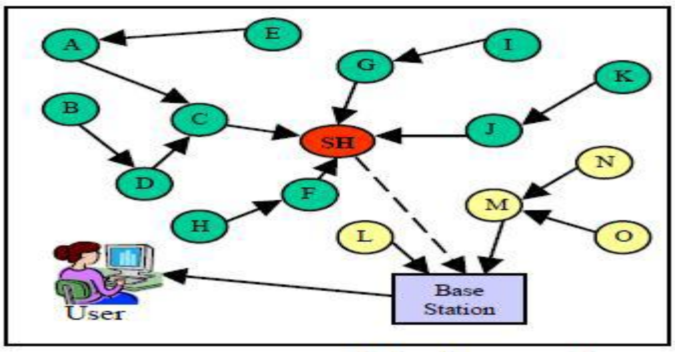


Figure 3: Sink hole attack

Sybil attack:

In the WSN the routing protocols assume that each node inside the network has a completely unique identification. In the Sybil attack [1], the attacker can look like in multiple locations at the identical time. This can be achieved by way of developing faux identities of nodes placed at the edge of the conversation variety. Multiple identities may be occupied in the sensor community either with the aid of fabrication or stealing the identities of valid nodes. Sybil assault is chance to geographic routing protocols. Location conscious routing regularly calls for to change coordinate statistics with their buddies to shape a network. So it expects nodes to be present with a unmarried set of coordinates, however through Sybil attack an attacker can” be multiple location at a time”. Since identity fraud ends in Sybil assault, right authentication can shield it. This attac occurs at network layer. This form of assault is feasible on flat based routing protocols, hierarchical routing protocols, vicinity primarily based routing protocols. The parent 4 demonstrates Sybil assault in which an attacker node ‘AD’ is gift with a couple of identities. ‘AD’ appears as node ‘F’ for ‘A’, ‘C’ for ‘B’ and ‘A’ as to ‘D’ so while ‘A’ wants to communicates with ‘F’ it sends the message to ‘AD’.

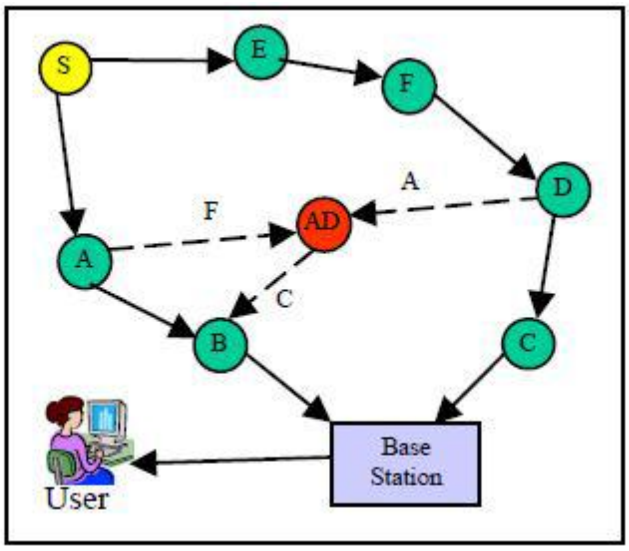


Figure 4: Sybil attack

HELLO flood attack:

Many protocols require to broadcast HELLO packets for neighbor discovery, and a node receiving such a packet may additionally anticipate that it is within radio variety of the sender. An attacker with large set up transmission electricity ought to persuade every node inside the community that the attacker is its neighbor, so that each one the nodes will reply to the HELLO message and waste their electricity. The result of a HELLO flood is that every node thinks the attacker is within one-hop radio verbal exchange variety. If the attackers finally put it up for sale low cost routes, nodes will tries to forward their message to the attacker. Protocols which depends on localization facts trade among acquaintances nodes for topology renovation or float control also are subjected to this assault. HELLO flood can also be thought of as one-way, broadcast wormhole. This attack may be averted via verifying the bi-directional of neighborhood links before the usage of them is effective if the attacker possesses the equal reception skills because the sensor devices. Another way by way of the use of authenticated broadcast protocols. This attack takes place at network layer in WSN. This attack is feasible on flat primarily based routing protocols, hierarchical routing protocols; area primarily based routing protocols, Network flow and QoS aware routing protocols. The determine 5 demonstrates how the attacker node ‘AD’ broadcast hiya packets to convince nodes in the community as neighbor of ‘AD’. Though a few nodes like I, H, F are a ways far from ‘AD’ they link ‘AD’ as their neighbor and try and forward packets, thru it which ends up in wastage of energy and facts loss.

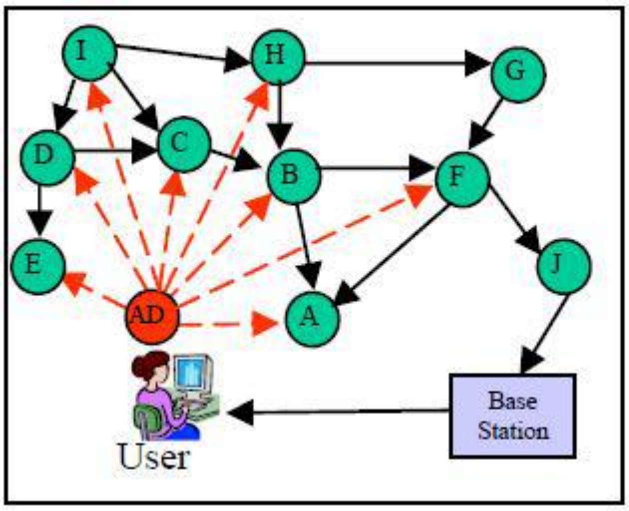


Figure 5: HELLO flood attack

Black hole attack:

The black hole assault [1] position a node in range of the sink and draws the entire visitors to be routed through it via marketing itself because the shortest direction. The attacker drops packets coming from precise assets in the network. This attack can isolate certain nodes from the bottom station and creates a discontinuity in community connectivity. This assault is simpler to locate than sink hollow attack. This assault commonly targets the flooding based protocols. Another thrilling sort of attack is homing. In a homing attack, the attacker looks at community visitors to infer the geographic region of vital nodes, which includes cluster heads or buddies of the bottom station. The attacker can then physically disable these nodes. This results in some other form of black hole attack. This assault targets to block the traffic to the sink and to provide a higher ground for launching different attacks like records integrity or sniffing. This attack may be prevented if we can restriction malicious node to join the network. Network setup segment need to be carried out in a comfy way. This assault is viable at bodily layer. This assault is viable on flat primarily based routing protocols, hierarchical protocols, location based routing protocols and Network flow and Qos aware routing protocols. In the parent 6 BH is the black hole which first convenes the network that it's miles the nearest node to base station and attracts the network to route facts through it. When it receives facts from neighboring nodes it drops them.

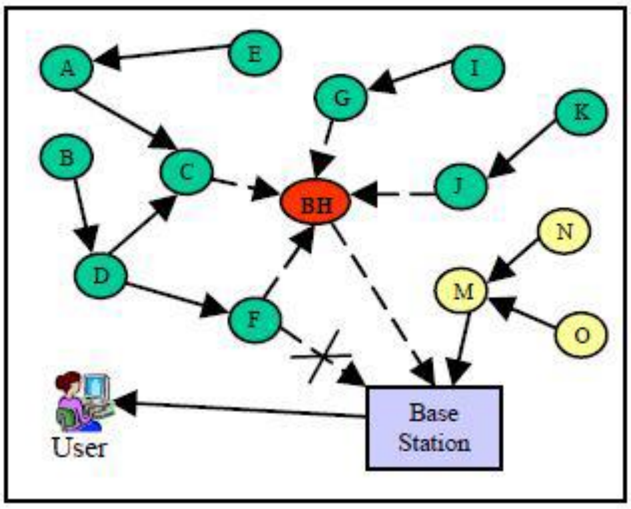


Figure 6: Black Hole attack

IV. Conclusion

- To avoid the Sybil attack in wireless sensor network we will implement solution on MATLAB. By using the encryption technique like **polynomial encryption**. In this techniques we are using following concepts like:
- Create a **hashing function**
- Using **merkle hash tree**

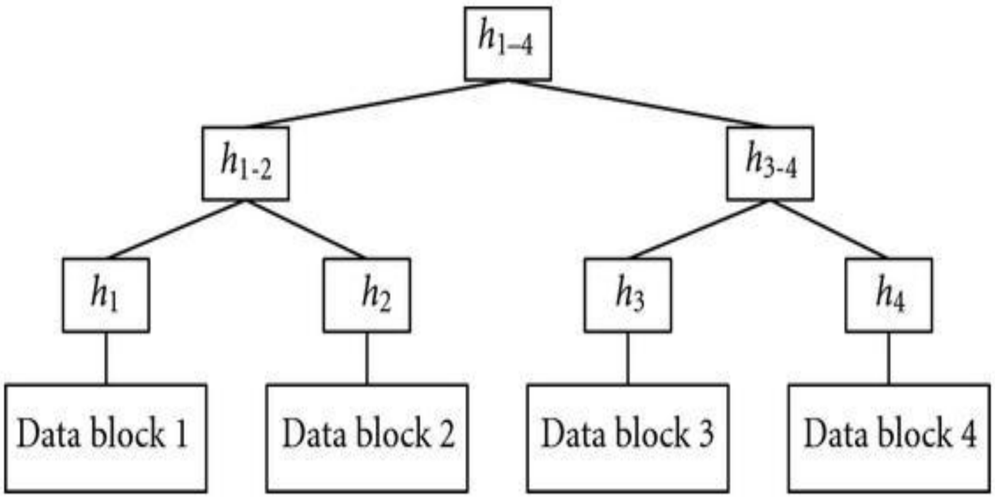


Figure 9: Merkle hash tree

- To avoid the Hello Flood attack in wireless sensor network so we are using the technique of **user interference –captcha code** (an acronym for "**Completely Automated Public Turing test to tell Computers and Humans Apart**") is a type of challenge-response test used in computing to determine whether or not the user is human. The term was coined in 2003 by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford to secure the wireless sensor network.

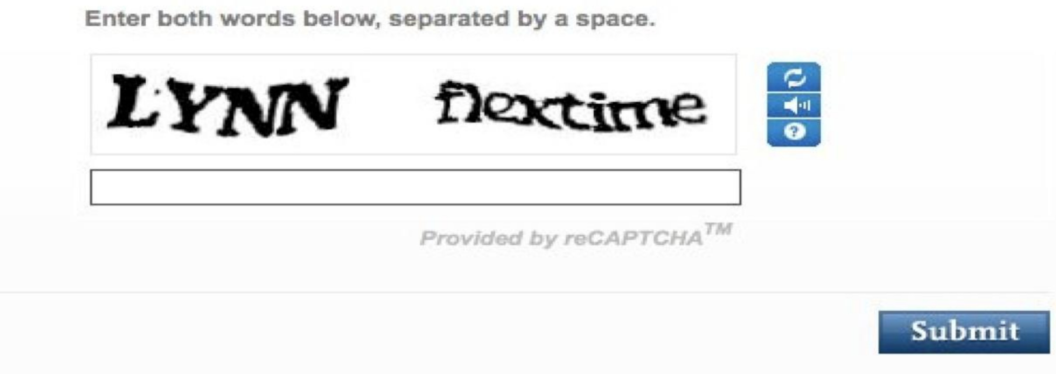


Figure 10: Captcha code

V. REFERENCES

[1] Zoran S.Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks", International Journal Of Communication, Issue 1, Volume 2, 2008

[2] Chris karlof and David wagner, "secure routing in wireless sensor network attacks and countermesures"

[3] A Hamid, S Hong, (2006) Defense against Lap-top Class Attacker in Wireless Sensor Network, ICACT

[4] A.M Riad et.al, "Secure Routing in Wireless Sensor Network A State of the Art", International journal of computer applications, volume 67- no.7, April 2013.

[5] S.Ganesh and R. Amutha, "Efficient & secure routing protocol for wsn through SNR based dynamic clustering mechanisms".

[6] Nasreen Fatima, "Review on the research evolution on secure routing in WSN "International journal of computer application, volume 119-no.17, June 2015.

[7] Ravindra gupta and hema dhadhal, "secure multipath routing in wireless sensor networks", International journal of electronics& computer science engineering, 1956.

[8] Michael Collins et. al., "A light weight secure architecture for wireless sensor network", Internet technology& secured transactions, vol.X no.X, 2008.

[9] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE International Workshop on Sensor Network Protocols and Applications, pages 113–127, May 2003.

[10] Jay dip sen, "A survey on wireless sensor network security", International journal of communication network & information security, vol. 1 No. 2, august 2009.

[11] Kuthadi venu madhav et.al. , "A study of security challenges in wireless sensor network", Journal of theoretical & applied information technology, 2005-2010.

[12] Aashima single and Ratika sachdeva, "Review on security issues& attacks in wireless sensor network", International journal of advanced research in computer science & software engineering, volume 3, Issues 4, April 2003.

[13] John Paul Walters et.al. , "Wireless Sensor Network Security: A Survey", Auerbach Publications, CRC Press, 2006.

[14] Adrian perrig, John stankovic, and David Wagner, "security in wireless sensor networks", communications of the ACM, Vol.47, No. 6, JUNE 2004.

[15] Vikash Kumar, Anshu Jain and P N Barwal, "Wireless Sensor Networks: Security Issues, Challenges and Solutions", International Journal of Information & Computation Technology, Volume 4, No 8, 2014.

[16] Mahfuzulhoq Chowdhury et.al. , "Security Issues in Wireless Sensor Networks: A Survey", International Journal of Future Generation Communication and Networking, Vol.6, No.5, 2013.

[17] Alok Ranjan Prusty, “The Network and Security Analysis for Wireless Sensor Network: A Survey”, International Journal of Computer Science and Information Technologies, Vol. 3, 2012.

[18] Santhosh Simon and K Paulose Jacob, “Energy Optimized Secure Routing Protocol for Wireless Sensor Networks”, International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 4, October 2013.

[19] Krishna Sampigethaya, “security of wireless sensor network enabled health monitoring for future airplanes”, 26th international congress of the aeronautical sciences, 2008.

[20] R. Brooks, P.Y. Govindaraju, M.Pireretti, N. Vijaykrishnan, and M. T. Kandemir, “ On the Detection Of Clones in Sensor Networks Using Random Key Predistribution, IEEE,pp. 1246-1258,2007.

[21] C. Blundo, A.D.Santis, A. HerzBerg, S. Kutten, U. Vaccro, and M. Yung. “Perfectly- Secure Key distribution for dynamic Conferences”, Information and Computation, pp. 1-23, 1998.

[22]C. Bekara and M. Laurent-Maknavicious. “A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks”, IEEE, pp.59-59, 2007.

[23] A. Agah, S. K. Das, K. Basu, and M. Asadi. “Intrusion detection in Sensor Networks: a Non-Cooperative Game Approach”, IEEE, pp. 343-346, 2004.

[24] Elmurod Talipov, Donxue Jin, Jaeyoun Jung, Ilkhyu Ha, YoungJun Choi, and Chong gun Kim, “Path Hopping Based Reverse AODV for Security”, Springer, pp. 574-577, 2006.

[25] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, “Security issued in Wireless Sensor Networks”, International journal Of Communications, Vol.2, Issue. 1, 2008.

[26] Shio Kumar Singh, M P Singh, and D K Singh, “Routing Protocols in Wireless Sensor Networks- A Survey”, IJCSES, Vol .1, No. 2, Nov 2010.

[27] Kemal Akkaya and Mohamed Younis, “A Survey on routing protocols for wireless sensor networks”, Elsevier, 2003.

[28] CHEE-YEE and SRIKANTA P. KUMAR, “Sensor Networks: Evolution, Opportunities, and challenges”, Proceeding of the IEEE, Vol.91, No.8, Aug 2003.

[29] Satapathy, S.S and Saran, N., “TREEPSI: tree based energy efficient protocol for sensor information”, Wireless and optical Communication Networks, IFIP international Conference, 2006

[30] Shio Kumar, M P Singh , and D K Singh, “ Routing Protocols In Wireless Sensor Networks-A Survey”,International Journal of Computer Science & Engineering Survey (IJCSES) Volume 1,November 2010