International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 9, September- 2014

Analysis of DoS Attack in Wireless Sensor Network

Black-Hole Attack

Meena Pundir
Student
Department Of Computer Science
Punjabi University
Patiala, India

Dr. Maninder Singh
Assistant Professor
Department Of Computer Science
Punjabi University
Patiala, India

***Abstract*—Security is a vital issue in a wireless sensor networks. This is because of the fact that such networks are basically placed in hostile environments like surveillance;it has many military applications also.Security not only deals with protecting the networks but also includes detection of various attacks and their prevention.This paper would focus mainly denial of service attack and its prevention measures .Further we would experiment with the help of simulator to test the validity of our results.**

Keywords—WSN; security;DoS attack; black hole attack; detection; prevention

I. INTRODUCTION

Wireless sensor networks (WSNs) are large-scale innovative networks. They consist of distributed, low-power, low-cost, autonomous small-size devices using sensors to co-operatively collect information through infrastructure less adhoc wireless network. Wireless sensor networks was developed and motivated by military applications such as battlefield surveillance. Wireless sensor networks are used in different areas such as environment and habitat monitoring, home automation, and traffic control. Security plays a very important role in wireless healthcare applications sensor network applications. Wireless sensor networks consist of unique challenges, so security techniques used in conventional networks cannot be directly applied to wireless sensor network due to its unique characteristics. At first, production cost of sensor nodes are very high since sensor networks consist of a large number of sensor nodes. Already it has been argued that the cost of a sensor node should be much less than one dollar in order for sensor networks to be feasible. So, most sensor nodes are resource saved in terms of energy, computation, memory and communication capabilities. Second, in public hostile environment nodes may be deployed due to this sensor nodes vulnerable to physical attacks by adversaries. Third, insecure wireless communication channel are used by sensor networks and consist of lackinfrastructure. Due to this, existing security mechanisms are inadequate in nature, and new approaches are desired.

II. SECURITY IN WIRELESS SENSOR NETWORK

A. *Security Goals*

Wireless sensor networks are vulnerable to many attacks due to the broadcast nature of transmission medium, resource limitation and sensor nodes and uncontrolled environment where they are left unattended. There are some goals of WSN which are as:

- Availability: It refers to the property of the network to continue provide services regardless of the state of the network. A denial of service attacks is based to attack this property.
- Integrity: Integrity guarantees that no modification, addition, deletion is done to the message; the altering of message can be malicious or accidental.
- Confidentiality: It grantees that the message cannot be even viewed in its original form by any unauthorized person.
- Authenticity: With the help of this property the parties prove their identities. This property ensures that the parties are genuine not impersonators.
- Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.
- Anonymity: All the information about the identity of a node should be kept private for privacy-preservation.

B. *Security Threats and Attacks in Wireless Sensor Network*

Sensor nodes, in a Wireless Sensor Network, are often deployed in unattended and extreme environments. Such WSN applications are more vulnerable to WSN security attacks.The attacks are discussed as follows [1]:

- **Eavesdropping or passive information gathering**
  The communication medium of WSN applications is an unsecure wireless channel. An adversary, present in the region, may be able to intercept the communication between two legitimate nodes passively if the information is exchanged in plaintext. The adversary may monitor the communication which can later be used to carry out more sophisticated attacks against the WSN.

- **Node malfunctioning**
  A legitimate sensor node may at some point work inefficiently in the network. Malfunctioning of the sensor node may include dropping data packets at a high rate, denying packet forwarding requests (if working as a relay device), and soon. Such nodes need immediate detection as these conditions may severely affect the overall network performance.

- **Denial of service (DoS)**
  DoS attack has various forms. Such an attack not only target disruption or interruption in network communication, but may also be used to temporarily weaken network capabilities to provide a service. Black whole, resource exhaustion, sinkhole, wormholes, flooding, induced routing loops, and so on are different types of DoS.

- **Node subversion**
  A true node if captured by an intruder may disclose all the encryption information, secret keys and algorithm to the some security-sensitive applications of WSN intruder. Secure communication of the WSN under attack can then be easily accessed by the attacker. The true node itself can be used as an attacker by the adversary to launch an insider attack. Such node may be successfully authorized and the attack may not be detected by the WSN at this point. This attack may lead to a high level of security breach and severe consequences.

- **Node outage**
  Some sensor nodes may work as relaying devices or routers Ina WSN. A legitimate sensor node or router might stop functioning due to many reasons, as a result of which communication may fail among parts of the WSN. The WSN must be able to robustly detect such node outage and should be able to act quickly and efficiently in determining alternative routes to achieve reliable end-to-end communication between communicating nodes in the network
  .

- **Message corruption**
  An intruder may be able to join the network and impersonate legitimate relaying node between two communicating trusted entities .Message integrity in this case may be attacked as the intruder may then be able to corrupt or modify the actual message contents resulting in a message corruption attack.

- **False node**
  An adversary may be able to add a sensor node to the network to misguide true nodes, exchange bogus data or corrupted data, block routes, and so on. This may lead to a communication bottleneck, false location claims, decrease in network performance, and so on. This is an extremely dangerous attack which may lead to severe network damage or even annihilation.

- **Node replication**
  An adversary may add a malicious node in the network by copying the identity of a true existing sensor node. This node may further bring severe damage to a WSN in various ways, including message corruption, injection of bogus data, misrouting information packets, and so on. Nevertheless, physical access to the network may compromise network secrets, security solutions; and so on .In security-sensitive applications of WSNs, the physical location information of a sensor node should not be disclosed to any unauthorized entity. Leakage of location information of sensor node may result in node compromise or node capture. If a legitimate sensor node is captured by an adversary, the secret cryptographic keys, encryption algorithms, and so on could be easily extracted by the attacker. This may allow the adversary to use this information in carrying out more sophisticated attacks on the WSN. These attacks may include false node, node replication, message corruption attacks, and so on.

A node capture attack is the most severe type of attack on a Wireless Sensor Network. Node capture attacks may be used to destroy the node completely. On the other hand, the attacker may modify the secure communication algorithm or cryptographic secret keys and inject the compromised node in the network, for example, adversary may compromise a relaying device to gather classified information in a surveillance network. The attacks discussed above mainly either lead to, or are carried out as, a result of node capture attack.

III. RELATED WORK

Due to the recent advancement in wireless communication like Bluetooth, a new concept of networking has emerged known as Wireless Sensor Networks (WSN). A wireless sensor network (WSN) consists of battery-operated sensor devices with computing, data processing, and communicating components. Wireless Networks provide a promising network infrastructure for many applications. S.H. Jokhio proposed DOS attack detection scheme SCADD.SCADD stands for sensor node capture attack detection and defense. SCADD protocol provides the security to the wireless sensor network by a cost effective solution. This is used for a secure sensitive applications. This mechanism is divided into two blocks: node attack detection block and defense advocating measure block. It is strategic-based attack detection to eliminate the misjudgment by using self-

destruction mechanism [1].Wireless sensor networks are very popular due to their applications. Due to the MEMS, Wireless Sensor Network manufacture low priced, low power multifunctional sensor node[2].There are many attack schemes tend to stop the performance of wireless sensor networks to delay or even prevent the delivery of data requested by user. In the term attack, an adversary's attempt to diminish or destroy a network. Denial-of-Service (DoS) attack refers to any event that eliminates a network's ability to perform its expected function [8]. This type of technique may be helpful in specific applications such as utilizing the best of these attacks to find the weak tips of presented protocols at different layers. With the help of understanding these vulnerabilities can develop techniques for identifying attacks and implement mechanisms to mitigate these attacks. Moreover, these networks at deployed in highly hostile environment like military for the surveillance in war zones, forest fire detection which poses many security risks. Zhang Yi Ying proposed new solution Mom for the detection and prevention of the Dos attack. Mom stands forMessage Observation Mechanism. MoM utilizes the similarity function to identify the content attack as well as the frequency attack. The MoM adopts rekey and reroute countermeasures to isolate the malicious node. The security analysis shows that our solution can not only detect and defense the DoS attack but also can reduce the energy consumption [10]. Alireja A. Nejhad give a solution of the problem depend on the nature of the traffic generated in the network as well as the capabilities of the adversary that must be resisted[11].There are various attacks are available in different layers of DoS and various solutions exist for their countermeasures [12].

IV. PROPOSED SOLUTION

Our solution is divided into two parts: the attack detection procedure and the attack prevention procedure. In attack detection procedure: we make a record of original value of each node. We set the threshold value. Compare original value with the thresh value of all nodes. Threshold value is the permissible value of parameters of node. If the actual value exceeds the threshold value it shows that an attack has taken place. In second part attack removal procedure we apply the node movement algorithm. We take the node out of sensing range of various other nodes and hence find another root for communication.

Flow Chart

There is a flow chart is given as Figure 1.1. According to the flow chart there are steps are given as:

Step1.At first step, we start with attack detection.

Step2.We check the original value of each node.

Step3. All original values of the all nodes are compared with the threshold value.

Step4. Now there is condition which decides the existence of malicious node in the network.

(a) If the threshold value of the node is greater than the actual value of the node it means there is no malicious node is found in the network.

(b)But if the condition is opposite, the actual value exceeds the threshold value, it means there is a malicious node found in the network.

Step5.If condition (b) executes then we apply node movement algorithm and to find a new route to reach the destination and continue process again.

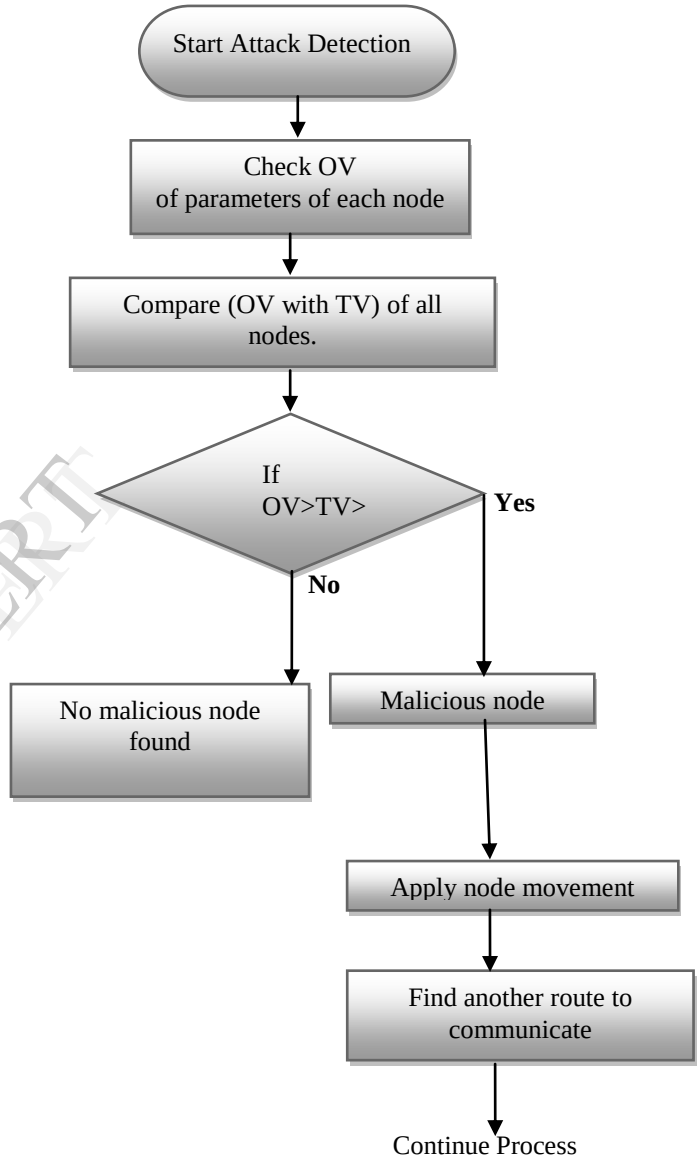

Figure 1.1

Simulation Parameter Setup

```
#==================================
#     Simulation parameters setup
#==================================
set val(chan)   Channel/WirelessChannel    ;# channel type
set val(prop)   Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)  Phy/WirelessPhy            ;# network interface type
set val(mac)    Mac/802_11                 ;# MAC type
set val(ifq)    Queue/DropTail/PriQueue    ;# interface queue type
set val(ll)     LL                         ;# link layer type
set val(ant)    Antenna/OmniAntenna        ;# antenna model
set val(ifqlen) 50                         ;# max packet in ifq
set val(nn)     5                          ;# number of mobilenodes
set val(rp)     AODV                       ;# routing protocol
set val(x)      607                      ;# X dimension of topography
set val(y)      586                      ;# Y dimension of topography
set val(stop)   10.0                        ;# time of simulation end
```

Figure 1.2

V. PERFORMANCE METRICS

(a)Packet Drop: It is defined as the total number of packets drops in the network with respect to the simulation time.

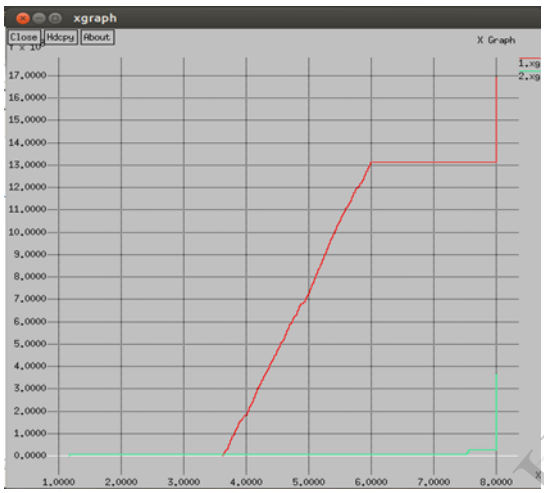

Fig 1.3 Comparison of Packet Drop with/without attack

(b)Packet Delivery Fraction: It is ratio of the number of delivered data packet to the destination.

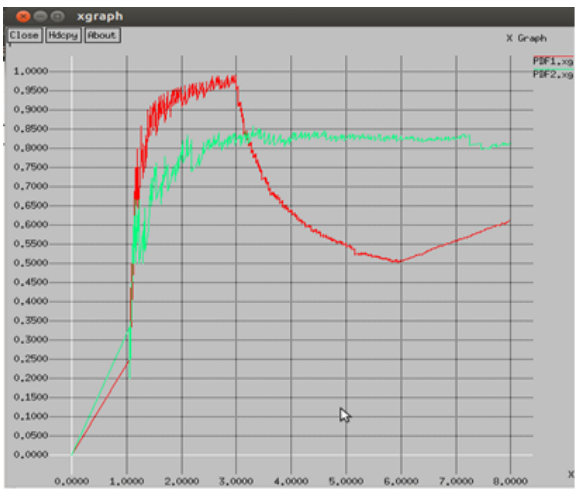

Fig 1.4 Comparison of Packet Delivery Fraction with/without attack

(c)Packet Delay: Packet delay is the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

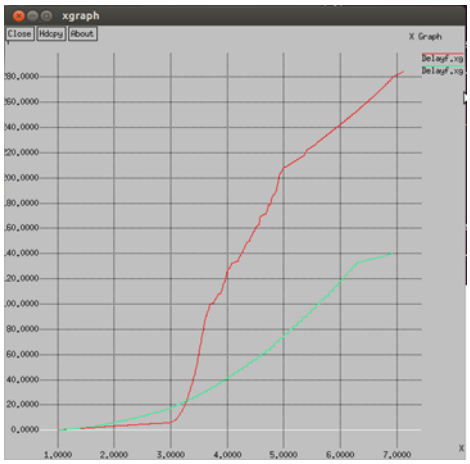

Fig 1.5Comparison of Packet Delay with/without attack

(d) Throughput: It is ratio of total number of delivered datapackets to the total duration of simulation time.

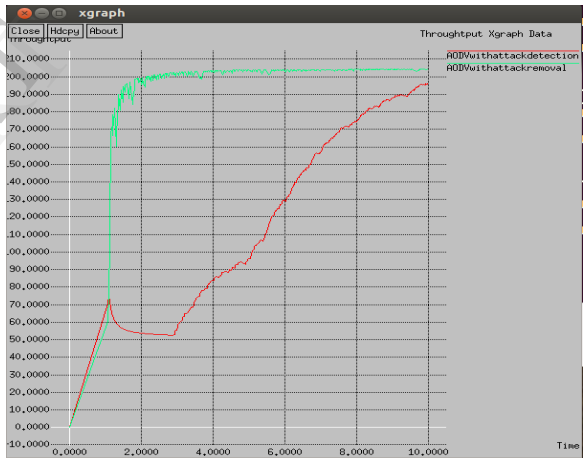

Fig 1.6Comparison of Throughput with/without attack

VI. CONCLUSION

In our paper we study and analyzed the effect of Black Hole Attack in an AODV Network. For this purpose, we implemented an AODV protocol that behaves as Black Hole in NS-2. Then we implemented a solution that tries to reduce the Black Hole effects in NS-2 and simulated the solution. Our simulation results are analyzed in which we saw that the packet drop is increased in the wireless sensor network. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the wireless sensor network. If the number of Black Hole Nodes is increased then the packet dropping is also expected to increase. The delay computation graph is also increased.

REFERENCES

[1] S.H Jokhio, I.A. Jokhio and A.H. Kemp, "Node capture attack detection and defense in wireless sensor networks", IET Wireless Sensor Systems, vol 2, pp. 161-169,2012.
[2] Xiaojiang Du and Hsiao-Hwa Chen, "Security in Wireless Sensor Network", IEEE Conference, 2008.
[3] Daniel-Ioan Curiac, Madalin Plastoi, Ovidiu Banias, Constantin Volosencu, Roxana Tudoroiu "Combined Malicious Node Discovery and Self-Destruction Technique for Wireless Sensors Network", IEEE Third International Conference on Sensor Technologies and Applications, pp 436-441, 2009.
[4] Tran Hoang Hai and Eui-Nam Huh, Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge", Seventh IEEE International Symposium on Network Computing and Applications, pp no. 325-331,2008.
[5] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International Conference ICACT 2006.
[6] Yong Wang, Garhan Attebury and Byrav Ramamurthy ,"A survey of security issues in Wireless Sensor Networks". IEEE Communication Survey , vol. 8, pp. 2- 22, 2006.
[7] Yi Qian, Kejie Lu and David Tipper," Towards Survivable and Secure Wireless Sensor Networks" IEEE Journal, vol.2, pp. 442-448, 2007.
[8] Yun Zhou, Yuguang Fang, and Yanchao Zhang, "Securing Wireless Sensor Networks: A Survey", IEEE Communication Surveys and tutorials, 3rd quarter journal, vol.2, pp.6-28, 2008.
[9] Zoran S. Bojkovic, Bojan M. Bakmaz and Miodrag R. Bakwaz, "Security Issues in Wireless Sensor Network", International Journal of Communication, Vol.2, pp.106-115, 2008.
[10] Zhang Yi-Ying, LI Xiang-zhen3, LIU Yuan-an, "The detection and defence of DoS attack for wireless sensor network",Journal ,pp no 52-56, 2012
[11] Alireza A. Nejhad , Ali Miri and Dimitris Makrakiset "Location privacy and anonymity preserving routing for wireless sensor networks", Journal,pp. 3433-3452,2008.
[12] Jaydip Sen, "Security in Wireless Sensor Networks". International Journal of Communication Networks and Information Security (IJCNIS), vol 1, pp. 56-78, 2009.
[13] Ivan Martinovic , Nicos Gollan, and Jens B. Schmitt, "Firewalling Wireless Sensor Networks: Security by wireless",IEEE Conference, pp. 770-777,2008.
[14] Maan Younis Abdullah, Gui Wei Hua, "Cluster-based Security for Wireless Sensor Networks", IEEE, International Conference on Communications and Mobile Computing,pp no. 555-559,2009.
[15] Dr. G. Padmavathi and Mrs. D. Shanmugapriya," A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, pp no 1-9,2009.
[16] Lance Doherty, Kristofer S. J. Pister, Laurent El Ghaoui,"Convex Position Estimation in Wireless Sensor Networks", IEEE International Conference, pp no. 1655-1663,2001.
[17] Tanveer A. Ziaand Albert Y. Zomaya,"A Lightweight Security Framework for Wireless Sensor Networks", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 2, number: 3, pp. 53-7,2006.
[18] Yan-Xiao Li, Lian-Qin and Qian-Liang, "Research on Wireless Sensor Network Security", IEEE, International Conference on Computational Intelligence & Security, pp. 493-496, 2010.
[19] Hero Modares, Rosli Salleh and Amirhossein Moravejosharieh, "Overview of security Issues in Wireless Sensor Networks", IEEE, Third International Conference on Computational Intelligence, modeling & simulation, pp. 308-311, 2011.
[20] Gaurav Sharma, Suman Bala, Anil K. Verma, "Security frameworks for Wireless Sensor Networks- Review", Elsevier, 2nd International Conference on Communication, Computing & Security [ICCCS-2012], 2012.
[21] Anand, M., Cronin, E., Sherr, M., Blaze, M., Ives, Z., Lee, I.: 'Sensor network security: more interesting than you think'. HOTSEC'06: Proc. First USENIX Workshop on Hot Topics in Security, USENIX Association, Berkeley, CA, USA, pp. 25–30, 2006.
[22] Hai, T.H., Huh, E.-N.: 'Detecting selective forwarding attacks in wireless sensor networks using two-hop neighbor knowledge'. IEEE International Symposium on Network Computing and Applications, pp. 325–331, 2008.
[23] Du, X., Chen, H.-H.: 'Security in wireless sensor networks', IEEE Wireless Communication, 15, (4), Journal,vol.2, pp. 60–66, 2008.
[24] Capkun, S., Hubaux, J.P.: 'Secure positioning of wireless devices with application to sensor networks'. Proc. IEEE 24th Annual Joint Conference on IEEE Computer and Communications Societies, INFOCOM, vol. 3, pp. 1917–1928, 2005.
[25] Ekici, E., Vural, S., McNair, J., Al-Abri, D.: 'Secure probabilistic location verification in randomly deployed wireless sensor networks', Ad Hoc Network, 6, (2), IEEE Journal vol.3,pp. 195–209, 2008.
[26] Zhang, Y. Liu, W., Fang, Y.: 'Secure localization in wireless sensor networks'. Military Communications Conference, MILCOM 2005, vol. 5, pp. 3169–3175, October 2005.
[27] Ren, K., Lou,W., Zeng, K., Moran, P.J.: 'On broadcast authentication in wireless sensor networks'. IEEE Transmission Wireless Communications, Vol. 6, Iss. 11, pp. 4136–4144, November 2007.
[28] Lazos, L., Serloc, P.R.: 'Secure range-independent localization for wireless sensor networks'. WiSe'04: Proc. Third ACM Workshop on Wireless Security, New York, NY, USA, pp. 21–30, 2004.
[29] K. Fall and K. Varadhan, "Editors ns Notes and Documentation," The VINT Project,UC Berkeley, LB,USC/ISI,and Xerox PARC, Nov.1997. Available: http://wwwmash.cs.berkeley.edu/ns.
[30] Aashima Singla and Ratika Sachdeva," Review on Security Issues and Attacks in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, vol 3, pp no. 529-534 ,2013.
[31] K.Venkatraman, J.Vijay Daniel, G.Murugaboopathi, "Various Attacks in Wireless Sensor Network: Survey", International Journal of Soft Computing and Engineering (IJSCE), Volume-3, Issue-1, pp no. 208-211, March 2013.
[32] L. N. Jyothi Bhargavi, J. Girija , "Removal of Black Hole Attack by Implementing Digital Signature and Trust Index Computation in Wireless Networks", International Journal of Scientific Engineering and Research (IJSER), vol 1, pp no. 136-140,2013.
[33] Ahmad Abed Alhameed Alkhatib, Gurvinder Singh Baicher," Wireless Sensor Network Architecture", International Conference on Computer Networks and Communication Systems,vol 35,pp no. 11-15,2012.
[34] Donggang Liu Peng Ning and Wenliang Du," Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks", IEEE International Conference on Distributed Computing Systems,pp no 1-11,2005.
[35] N. Vlajic and D. Xia, "Wireless Sensor Networks: To Cluster or Not To Cluster?",IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06),pp no 1-9, 2006.