iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VIII **Month of publication:** August 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

To maintain data consistency in Cooperative Caching Based Energy Efficient Protocol in WSN

Kirandeep Kaur[1], Ranbir Singh Batth[2]
M.Tech (CSE) Student, Assistant Professor
SUS College of Engineering and Technology, Mohali

Abstract: A sensor node commonly consists of sensors, actuators, memory, a processor and they also have communication ability. There is an issue of energy efficiency in Wireless Sensor Networks. First of all cooperative caching is merge with the existing algorithm. But this scheme has some problems also. So to overcome it pull and push based technique will be proposed. In our proposed work we will overcome the problem of dropped packet by detecting them and redirect to the source with the help of monitoring nodes.

Keywords: Sensors, Base station, Dissemination nodes, attack

I. INTRODUCTION

A wireless sensor network is made up of a large number of nodes which spread over a definite area where we want to look after at the changes going on there[2].A sensor node generally have sensors, actuators , memory, a processor and they do have communication ability. All these sensor nodes are allowed to communicate through a wireless medium. The wireless medium may either of radio frequencies, infrared or any other medium, of course, having no wired connection. These nodes are deployed in a random fashion and they can communicate among themselves to make an ad-hoc network [7]. If the node is notable to communicate with other through direct link, i.e. they are out of coverage area of each other; the data can be send to the other node which lie in between them. This is referred to as multi-hoping [9]. All sensor nodes work cooperatively to serve the requests. WSNs use peer-to-peer communication between the nodes so they are not centralized. So prior establishment is not required. Infrastructure to deploys the network. It includes two kinds of nodes. Sensor nodes with limited energy can sense their own residual energy and have the same architecture. One Base Station (BS) without energy restriction is far away from the area of sensor nodes. All sensor nodes are immobile. They use the direct transmission or multi-hop transmission to communicate with the base station. Sensor nodes sense environment at a fixed rate and always have data to send to the base station. Sensor nodes can revise the transmission power of wireless transmitter according to the distance [6]. There are different types of attacks can be possible in wireless sensor networks. Cloning attack is the opening point to a large span of insidious attacks such attack, a rival uses the credentials of a compromised node secretly introduce replicas of that node into the network [8].In Sinkhole Attack**,** attackers tries to attract the traffic from a fastidious region through it when it has some comprehension of routing protocols. In wormhole attack, a malicious node, at one location in the network receives packets and to another location in the network tunnels them, to the location where packets are present into the network. Similarly black hole attack is also possible in wireless sensor network. In this paper we introduced different types of attacks in wireless sensor networks. In section 2nd we will do literature survey. In section 3rd we will introduced about black hole attack in wireless sensor networks. In section 4thproblem formulation will be discuss.

II. REVIEW OF LITERATURE

Virendra Pal Singh (2010) et.al presented [1] that wireless sensor network have emerged as a vital function of the ad-hoc networks model for monitoring physical environment. But sensor networks mostly have boundaries like battery power, communication range and processing ability. Networks become vulnerable to various attacks because of Low processing power and wireless connectivity. One of these attacks is hello flood attack, in which an challenger, which is not a official node in the network, send hello request to any legal node and break the safety of WSN. The existing solutions for these attacks are mainly cryptographic, which have high computational complexity. Thus they are not much suitable for wireless sensor networks. In the given paper a technique based on signal strength has been projected for detecting and preventing hello flood attack. Nodes first classified as frien

ds and strangers with a technique based on the signal strength. The Short client puzzles which requires less computational power and battery power are used to confirm the legality of distrustful nodes.

Dr. G. Padmavathi and Mrs. D. Shanmugapriya (2009) discussed [2] that wireless Sensor networks (WSN) is an up-and-coming technology and have vast potential to be engaged in serious situations such as battlefields and commercial applications like buildings, traffic inspection, habitation monitoring and smart homes and also for numerous other scenarios. One of the major challenges which wireless sensor networks face today is safety measures. While the employment of sensor nodes in an unattended location makes the networks at risk to a variety of potential attacks, the intrinsic power and limitations of memory of sensor nodes makes usual security solutions unachievable. The sense technology united with the processing power as well as with wireless communication makes it advantageous for being oppressed in great quantity in future. This paper discusses a variety of attacks in WSN and their classification mechanisms and diverse securities accessible to handle them together with the challenges faced.

Kalpana Sharma and M K Ghose (2010) introduced[3] that Wireless sensor networks have turn out to be a growing area of delve into and expansion due to the fabulous number of applications that can greatly promote from such systems and lead to the growth of minute, inexpensive, disposable and self controlled battery powered computers, known as sensor nodes or "motes", which accept input from an attached sensor, process the input data and broadcast the results wirelessly to the transit network regardless of making such sensor networks possible, the wireless sensors have a number of security threats when deployed for various applications like military surveillances etc . The wireless nature of sensor networks and the security architectures creates the various security problems. Wireless sensor networks also have an additional vulnerability because of the hostile placements of the nodes as they can't be physically protected. In this paper some safety threats and challenges faced by WSNs are discussed. An abstract of the WSNs threats affecting diverse layers along with their security mechanism is presented. It is concluded that the defense mechanism presented only gives strategy about the WSN security threats; but the solution depends on the type of application for which WSN is deployed for. There are many security mechanisms which are used in "layer-by-layer" basis as a security device. Lately researchers are working for integrated system for security in place of focusing on different layers independently. Through this paper the most common security threats are presented in a range of layers and their most possible solutions.

Chris Karlof, David Wagner (2003) considered [4] the routing security in wireless sensor networks. A variety of sensor network routing protocols have been proposed but they are not planned for security goals. They projected security goals for routing in wireless networks and illustrate how attacks in opposition to ad-hoc and peer-to-peer networks can be modified into powerful attacks against sensor networks, bring in two classes of novel attacks in opposition to sensor networks like sinkholes and HELLO flood attacks, and study the security of the whole sensor network routing protocols. The crippling attacks are described against all of them and suggest various countermeasures with design considerations. This examination is the first one for secure routing in sensor networks.

Ju young Kim and Ronnie D. Caytiles (2005) presented [5] a study of the different vulnerabilities, threats and attacks for Wireless Sensor Networks. Effectual management of the threats related with wireless technology requires a proper and through consideration of risk given in the setting and improvement of a plan to diminish acknowledged threats. An analysis to help network managers recognize and review the various threats linked with the use of wireless technology and various available solutions for countering those threats are discussed. Wireless Sensor Networks provide a numerous opportunities for increasing productivity and minimizing costs. It provides significant advantages for many applications that would not have been possible for the past. The unlike vulnerabilities, threats and attacks that could possibly put WSNs in a vital or critical situation have been recognized and discussed in this paper. The different categories for these threats are defined to identify a possible countermeasure scheme applicable for each threat classification.

III. BLACK HOLE ATTACK IN WIRELESS SENSOR NETWORK

Volume 3 Issue VIII, August 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

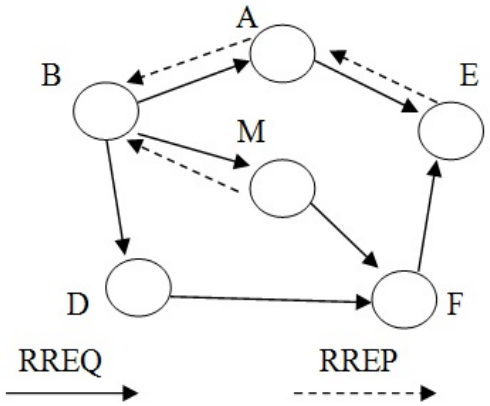


Fig. 1: Routing Discovery Process in AODV protocol

A black hole problem means that a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. Imagine a malicious node 'M'. When node 'A' broadcasts a RREQ (Route Request) packet, nodes 'B' 'D' and 'M' receive it. Node 'M', is a malicious node, so it does not check its routing table for the route requested to node 'E'. Hence, it immediately sends back a RREP (Route Reply) packet, claiming a route to the destination. Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'. Node 'A' assumes that the route through 'M' is the shortest and it sends any packet to the destination through this route. When the node 'A' sends data to 'M', it does not sends the data further and thus behaves like a 'Black hole'.

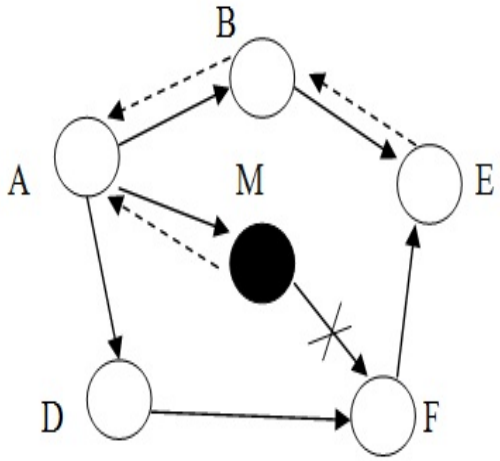


Fig. 2: Black Hole Attack in AODV protocol

In AODV (Ad hoc On Demand Distance Vector), the sequence number is used to determine the originality of routing information restricted in the message from the originating node [10]. When RREP (Route Request) message is generated, a destination node compares its recent sequence number, and the sequence number in the RREQ (Route Request) packet plus one, and then the larger one is selected as RREPs (Route Request) sequence number. After receiving a number of RREP (Route Request), the source node selects the greatest sequence number in order to construct a route. But, in the presence of black hole when a source node broadcasts the RREQ (Route Request) message for any destination, the black hole node instantly responds with an RREP (Route Request) message that includes the maximum sequence number and this message is perceived as if it is coming from the destination or from a node which has a new enough route to the destination [11]. The source then starts to send out its packets to the black hole believing that these packets will reach the destination. Thus the black hole catches all the packets from the source and in place of forwarding those packets to the destination it will simply discard those packets Thus the packets attracted by the black hole node will not arrive at the desti natio

n [12].

IV. PROBLEM FORMULATION

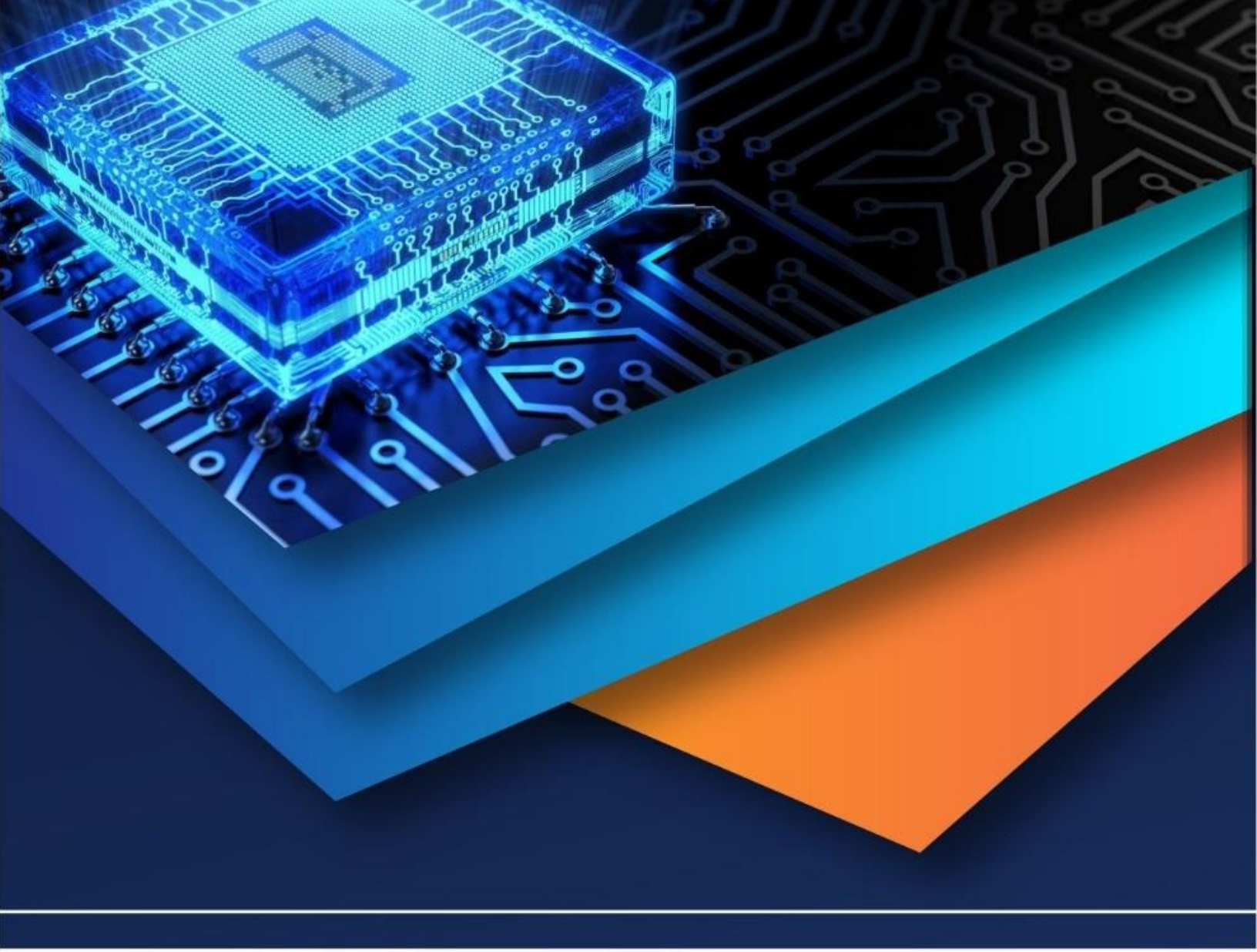
The present work is about the multi-sink data communication in wireless sensor networks. Now days, in the WSN if a user wants to communicate with the other nodes, the user firstly communicate to the sink. Then sink communicate to the IDN, IDN stands for intermediate dissemination node. The node further sends the request to other IDN and so on. Hence whatever the information a user wants to know is done only via the IDN. In this communication the energy consumption is very high due to malicious node. Hence the battery life of the node is also less. Hence the failure in the communication is occur, which leads to the big problem. There are number of finite nodes in the network. First of all clusters are formed a using LEACH or HEAP. After that clusters head are formed in each cluster. There is a sink which is available at the network and directly communicate with decimate node. One decimate node is also present at the center of the network which communicate with sink and all other cluster heads also for the data exchange. Suppose there is also a second network. To communicate with that network inter decimate nodes are require. There is a malicious node which is present at one of the cluster which triggers black hole attack. When decimate node sends data to inter decimate which is malicious node than packet drop problem occur. There is no data exchange between both networks so inconsistency problem arises. This problem will degrade the performance of the network.

V. CONCLUSION

In this paper, it is concluded that there is a problem of existing algorithm. So to overcome this cooperative caching scheme will be applied with it. To make it more efficient push and pull technique. The proposed technique will be more efficient and reliable as compare to existing technique.

REFERENCES

[1] Virendra Pal SinghSweta Jain and Jyoti Singhai, “Hello Flood Attack and its Countermeasures in Wireless Sensor Networks”, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010
[2] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009
[3] Kalpana Sharma and M K Ghose, “Wireless Sensor Networks: An Overview on its Security Threats” IJCA Special Issue on “Mobile Ad-hoc Networks”MANETs, 2010
[4] Chris Karlof , David Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures” Elsevier, 2003
[5] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, “A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks” Journal of Security Engineering, 2014
[6]TEODOR-GRIGORE LUPU, “Main Types of Attacks in Wireless Sensor Network”, Recent Advances in Signals and Systems, ISSN: 1790-5109
[7] Arun K. Somani, Shubha Kher, Paul Speck, and Jinran Chen, “Distributed Dynamic Clustering Algorithm in Uneven Distributed Wireless Sensor Network” , 2006
[8] Amir Shiri et.al “New Active Caching Method to Guarantee Desired Communication Reliability in Wireless Sensor Networks” 2012
[9] Md Ashiqur Rahman and Sajid Hussain “Effective Caching in Wireless Sensor Network” 2007
[10] Sherrin J. Isaac, Gerhard P. Hancke , “A Survey of Wireless Sensor Network Applications from a Power Utility’s Distribution Perspective” ,2006
[11]Naveen Chauhan, “Cluster Based Efficient Caching Technique for Wireless Sensor Networks” , (ICLCT'2012)
[12] Mudasser Iqbal, “An Energy-Aware Dynamic Clustering Algorithm for Load Balancing in Wireless Sensor Networks”, JOURNAL OF COMMUNICATIONS, VOL. 1, NO. 3, JUNE 2006



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY