IJITKM 0973-4414 Volume-9, Number-1 Jun-Dec 2015 pp. 1-5 **Impact Factor 2.8** available online at www.csjournalss.com

A Novel Technique to detect a black hole attack on the malicious Immediate Dissemination Node in Cooperative Caching based scheme

Kirandeep Kaur[1], Ranbir Singh Batth[2]
[1]M.Tech (CSE) Student, SUS College of Engineering and Technology, Mohali
[2]Assistant Professor, SUS College of Engineering and Technology, Mohali
kiran.kohli10@yahoo.in, batth.ranbir@gmail.com

Abstract: Mobile Sensor networks have mobile sensor nodes. These sensor networks have various issues like constrained energy resources and various security issues. In this paper, we identify a black hole attack in cache cooperative technique and then isolate it by proposing a novel technique which increases the performance of the system.
Keywords: Sensors, Base Stations, Cooperative Caching, Cache.

1. Introduction

1.1 WSN: A wireless sensor network is a collection of various nodes which are attached with each other without any of the centralized node. In today's era, wireless sensor networks are becoming very vital in various fields that's why it becomes a trend to work with wireless sensor networks. Wireless sensor networks use various communication protocols like carrier sense protocol for synchronization which are similar to the Ethernet standard. The various nodes in
wireless sensor networks share the same frequency and space by using these protocols. In wireless sensor network is a shared media because all users share the available bandwidth. The term wireless networks is mostly used for telecommunication networks where the interconnection between the nodes is without the use of any kind of wires and the example of such kind of telecommunication networks is computer networks. Wireless sensor networks are mainly consists of two components. One is the wireless access point which are the base stations attached with the wired networks and act as a middle man between wired and wireless networks. The other one are the wireless clients which are the network interfaces which communicate with the access points. Wireless sensor networks provide a reliable communication between the various wireless networks. Wireless sensor networks are self configured networks.

1.2 Cooperative Caching: Multiple sensor nodes in cooperative caching share and coordinate the cache data to reduce the communication cost and to take the advantage of collective cache space of cooperating sensors. Every sensor node has a modest local storage capacity linked with it which is known as flash memory which has several gigabytes storage capacity. Every sensor node has a non-volatile memory like flash memory which stores i.e. caches all the repeatedly accessed data items and it then satisfies not only the node's own requests but also the requests of the other nodes. When any data is not available in the local cache, it is first searched in its zone before forwarding it to the next node which lies in the path towards the data source. This process of cache admission control relies on the distance criteria of a nod from the sink and the main concern is given to the nodes which are located near the sink. By using a Cooperative caching technique we can handle the requests because it helps to reduce availability, decrease the requirements for bandwidth and it decides which data should be cached or not in wireless sensor networks. Cooperative caching scheme is used with a 2-D geometry sensor fields.

1.3 Security: Security is one of the major issuers in Wireless sensor networks. Wireless sensor networks are prone to numerous attacks which are based on secrecy and authentication, network availability and stealthy attacks against service integrity. The various types of attacks in wireless sensor networks are sinkhole attacks, Jamming, Wormhole attack, Sybil attack and Black hole attack.

1.3.1 Sinkhole attack: Sinkhole attack route the data packet by attracting it to the compromised node from the various neighboring nodes and then the packets are dropped or modified or spoofed. In this manner, sinkhole attack give rise to various attacks like selective forwarding, blackhole attacks and many more.

1.3.2 Sybil attack: Under this types of attacks, the various identities of the nodes are created to mislead the neighboring nodes while detection, formation of routes as well as topology maintenance.

1.3.3 Wormhole attack: A link is made by a single node forwarding messages between two adjacent but non-neighboring nodes or between pair of nodes placed at different parts of networks which are communicating with each other. The malicious node, receives packets and then tunnel them where to the locations where packets are present. It is a network layer attack and also very difficult to detect.

2. Review of Literature

Virendra Pal Singh (2010) et.al presented [1] that wireless sensor network have emerged as a essential role of the ad-hoc networks model for working in physical environment. But sensor networks frequently have limitations similar to battery power, communication range along with processing ability. Networks turn out to be defenseless to a range of attacks for the reason that of Low processing power as well as wireless connectivity. One of these attacks is hello flood attack, in which a challenger, which is not a official node in the network, send hello request to any permissible node and crack the security of WSN. The obtainable solutions for these attacks are largely cryptographic, which are having high computational complexity. Thus they are not greatly appropriate for wireless sensor networks. In the given paper a method based on signal strength has been projected for detecting plus preventing hello flood attack. Nodes primarily classify as friends and strangers with a method based on the signal strength. The Short client puzzles which requires less computational power as well as battery power are used to authenticate the validity of doubting nodes.

Dr. G. Padmavathi and Mrs. D. Shanmugapriya (2009) discussed [2] that wireless Sensor networks (WSN) is an up-coming technology and have immense prospective to be occupied in stern situations like battlefields and commercial applications similar to buildings, traffic inspection, habitation monitoring and smart homes and too for abundant other scenarios. The main challenge which wireless sensor networks have to face at present is safety actions. Although the deployment of sensor nodes in an unattended position makes the networks at risk to a range of potential attacks, the fundamental power and boundaries of memory of sensor nodes makes common security solutions inaccessible. The sense technology combined with the processing power along with wireless communication makes it helpful for being exploited in large extent in upcoming time. This paper tells various attacks in WSN and their categorization mechanisms and various securities available to handle them mutually with the challenges faced.

Kalpana Sharma and M K Ghose (2010) introduced[3] that Wireless sensor networks have turn out to be a rising area of research into and spreading out due to the marvelous number of applications that can wholly advance from such systems and direct to the development of minute, low-cost, disposable and self controlled battery powered computers called sensor nodes or “motes”, which recognize input from an attached sensor, process the input data and broadcast the outcomes wirelessly to the transfer network regardless of making such sensor networks achievable, the wireless sensors have a numerous security fear when deployed for diverse applications like military surveillances etc . The wireless character of sensor networks and the security architectures creates a range of security problems. Wireless sensor networks also have a further weakness for the reason of the hostile placements of the nodes as they can’t be protected physically. In this paper several safety threats and challenges in WSNs are discussed. An intangible of the WSNs threats upsetting various layers along with their security mechanism is offered. It is accomplished that the defense mechanism discussed 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 loads of security mechanisms which are used in “layer-by-layer” basis as a security mechanism. Recently researchers are functioning for integrated system for security in position of focusing on diverse layers in parallel. In the course of this paper the main familiar security threats are offered in a range of layers and their largest part feasible solutions.

Chris Karlof, David Wagner (2003) considered [4] the routing security in wireless sensor networks. A sort 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 customized 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 dissimilar vulnerabilities, threats and attacks that could possibly put WSNs in an essential or critical situation have been recognized and discussed in this paper. The diverse categories for these threats are defined to recognize a possible countermeasure scheme applicable for each threat classification.

3. Black Hole Attack In Wireless Sensor Network

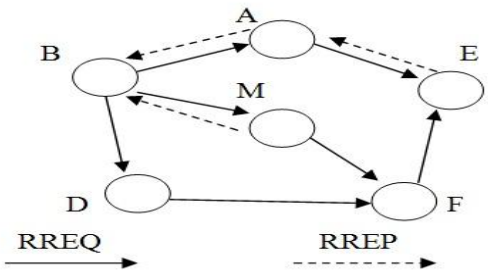

Fig. 1: Routing Discovery Process in AODV protocol

A black hole problem means that a malicious node utilizes the routing protocol to declare 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'.

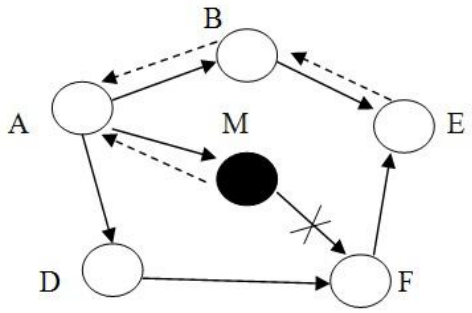

Fig. 1.1: Black Hole Attack in AODV protocol

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 destination [12].

4. Proposed Technology

In Wireless Sensor Networks, a communication between users and the other nodes is done using a sink node. Then the sink node communicate to the Immediate Dissemination Node and then to further Immediate Dissemination Nodes. Due to degradation of battery in the networks, Cooperative Caching technique is used in which the sensed data is cached at the caching nodes. The sink node sends requests to the caching nodes and then the caching nodes respond back. In the network the blackhole attack is triggered by the malicious nodes. These nodes send wrong information about the path to the source and then drops all the packets and acts like a blackhole. So the node registration method is used to overcome this problem. In this method, the nodes register

themselves to the base station or sink and then the sink verifies the nodes registration and if the node is not verified it is detected as a malicious node.

5. Experimental Results

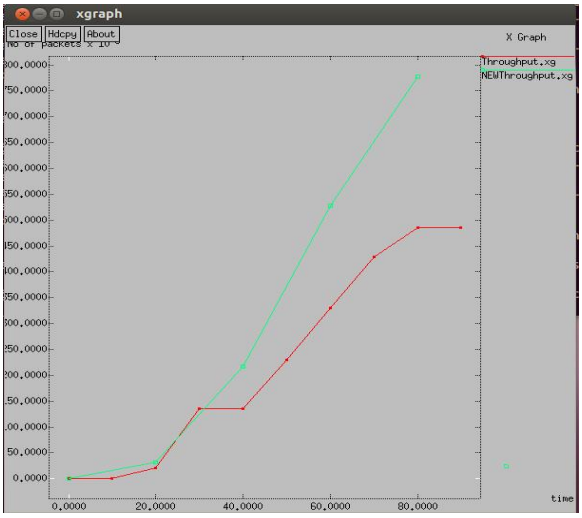

Fig.1.1: Comparison between Throughput at the time of attack and after avoidance of attack

X axis shows time in seconds and Y axis shows no. of packets. Above figure shows that throughput is more after the avoidance of attack as compared to lesser throughput at the time of attack. Here, Green line shows increased throughput after the avoidance of attack and red line shows lesser throughput at the time of attack.

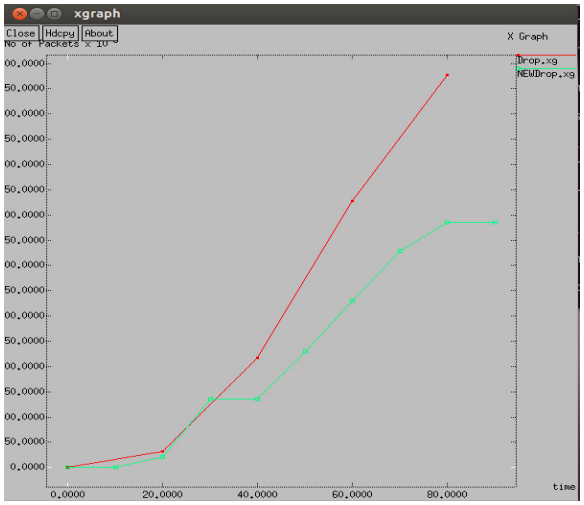

Fig.1.2: Comparison between Packet Drop at the time of attack and after avoidance of attack

Packet Drop is defined as total number of packets dropped during simulation. Above figure shows that packet drop are less after the avoidance of attack as compared to greater number of packets drop at the time of attack. X axis shows time in seconds and Y axis shows no. of packets. Here, Green line shows lower number of packets drop after the avoidance of attack and red line shows more packets drop at the time of attack.

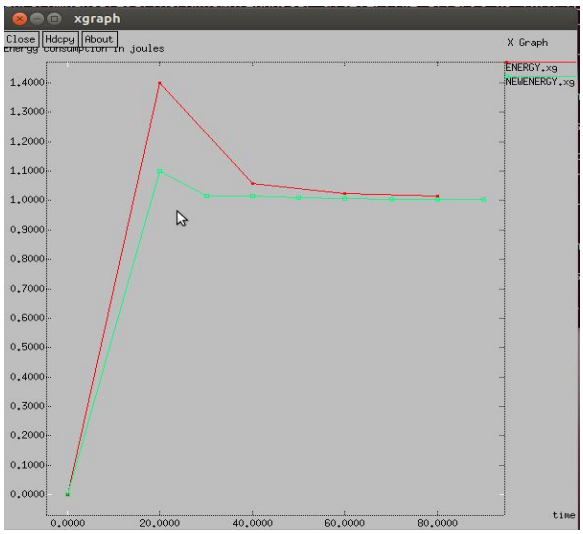

Fig.1.3: Comparison between Energy consumption at the time of attack and after avoidance of attack

Above figure shows that energy consumption is less after the avoidance of attack as compared to greater energy consumption at the time of attack. X axis shows time in seconds and Y axis shows energy consumption in Joules. Here, Green line shows lesser energy consumption after the avoidance of attack and red line shows greater energy consumption at the time of attack.

6. Conclusion

A new technique is proposed to remove the inconsistency of the network and thus increases the reliability of the network by detecting and then isolating the malicious nodes which triggers the black hole attack. This technique is based on the node registration method. This malicious node degrades the performances of the networks so these are first detected and then isolated from the network if they are failed to register themselves to the sink node. In this paper, a new technique is proposed which is more efficient as it increases the performance of the system.

References

[1] Virendra Pal Singh, Sweta 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 andChallenges in Wireless Sensor Networks",* International Journal ofComputer 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, ShubhaKher, 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] MdAshiqurRahman and SajidHussain"*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] MudasserIqbal, "*An Energy-Aware Dynamic Clustering Algorithm for Load Balancing in Wireless Sensor Networks",* JOURNAL OF COMMUNICATIONS, VOL. 1, NO. 3, JUNE 2006