November-December 2019
ISSN: 0193-4120 Page No. 4724 - 4727

Black Hole and Grey Hole Detection in WSN using DSR Protocol

Gayathiri.M,
Student, Dept. Computer Technology(CT), Sri Krishna arts and science College, Coimbatore, Tamilnadu, India. (E-mail: gayathirim18mct005@skasc.ac.in)

Nandhini.S,
Dept. Computer Technology(CT), Sri Krishna arts and science College, Coimbatore, Tamilnadu, India. (E-mail: nandhinis@skasc.ac.in)

Swathy.R,
Student, Dept. Computer Technology(CT), Sri Krishna arts and science College, Coimbatore, Tamilnadu, India. (E-mail: swathyr18bct050@skasc.ac.in)

Swetha.S,
Student, Dept. Computer Technology(CT), Sri Krishna arts and science College, Coimbatore, Tamilnadu, India.(E-mail: swethas18bct052@skasc.ac.in)

Article Info
Volume 81
Page Number: 4724 - 4727
Publication Issue:
November-December 2019

Article History

Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *23 December 2019*

Abstract

In this paper, a low energy efficient hierarchical clustering and routing protocol based on the Genetic Algorithm (LECR-GA) for marine networks is proposed, which uses clustering and routing algorithms to efficiently intensify the lifespan and to enhance the quality of service (QoS) parameters. The proposed algorithm's operation divided into two rounds which extend the lifetime of marine networks by selecting the optimum cluster head (CH) and the shortest route for sending the aggregate data at a base station (BS) to save the energy. The efficient energy optimization is successfully achieved by using LECR-GA as the performance of LECR with GA protocol has remarkable abatement in terms of energy consumption rather than simple without GA. Network simulator2.35 is used to examine the performance of the LECR-GA protocol for marine networks in-terms of parameters such as delay, packets received at BS and throughput.

Keywords: *Energy optimization, Marine Network, NS2.35, , Routing and Clustering protocol.*

I. INTRODUCTION

Various varieties of attacks exist like:

- Passive Eavesdropping
- Selective Existence (Selfish Nodes)
- Grey Hole Attack (Routing Misbehaviour)
- Black Hole Attack
- Modification Attack
- Attack in oppose of Routing Tables
- Torture Sleep Deprivation Attack (Battery Exhaustion)

One of the foremost common routing protocols attacks on the currently a days-Grey hole and region attack. A region may be a unwanted node which draws all other traffic within the group of hubs by finding some nearest way in the network. The similar Region puts all other packets it gains(receives) from the corresponding opposite nodes. In very region atttacks, unwanted nodes don't send acquired management mesages .In the grey hole attack, more malicious node or nasty node is acting as traditional nodes & leaves the unique mesages or packets that goes passing them,

November-December 2019
ISSN: 0193-4120 Page No. 4724 - 4727

thus activity the necessary infos to go before the subsequent node or final point node. A grey hole attack effects within the network as one or two nodes, and also a region attack affects the full networks .

II. CONTRIBUTION OF MANET & AODV

Mobile ad-hoc network (MANET) is suburbanized system, during this system hubs will move increasingly. OSI Network layer faces many attack . Grey hole attack chip away at the most notable succession variety amid Replay message, a gathering of grey hole hubs effectively utilised against steering in MANET known as community grey hole attack. Here existing algorithmic program accustomed AODV (Ad hoc Ondemand Distinct Vector).Existing AODV is associate degree ondemand or reaactive routing protocol. In AODV, once a route require a new destination route, a supply node generates a route request (RREQ) packet to seek out a route to the final destination node. A sound route will find once a RREQ attains a final destination node either itself, or associate degree on middle node with a contemporary route to the destination node. A contemporary route could be a valid route entry for the destination node whose associated sequence variety is larger than sequence variety of RREQ packet. A route is created on the market to control the singular cast on a route reply (RREP) packet to a supply node. A RREP packet is singular cast by a destination or associate degree middle part of the node. Once a link segment in a very route is acquired, a route err (RERR) packet is employed for the gain apprize alternative collaborating node.

III. LITERATURE SURVEY& RESULTS

TITLE	AUTHOR	METHOD	YEAR	DESCRIPTION
Grey hole And Black hole Attack Identification And Prevention Using Ip Backtracking In WSN	Shaifu, AmandeepKaurVirk	IP Backtracking in WSN	2017	Proposed a mechanism that takes an control to track a approach for multi purposetrase-back by which all the other gain marking and packet work square measure integrate for detection of grey holeattack.
”Performance in Evaluating the Attack Detecting Algorithms On Delay Tolerantt Networks”	ChaaudhariRajashrii M., Patilmanesh P.	Delay Tolerant Networks	2017	Proposed the mechanism for detection of part and grey hole attackers supported statistical-based detection of part and grey hole attackers (SDBG).
A Secured Multicast Routing Protocol Against Grey Hole Attack	GeetanjaliRathee And HemrajSaini	Routing Protocol Multicasting	2016	Proposed a detection mechanism of grey hole attack and make sure the security against grey hole attack by shrewd the each node delivery a packet to proportion of each delivery node and if the node having less proportion of packet delivery than the predefined threshold price (i.e. 97%) is taken into account as grey hole or malicious node
Detecting In Mittigation Of Grey	BANSI S. KANTARIYA1,	Network Using Trust	2013	Suggested a trust mechanism to notice the grey hole attack,

November-December 2019
ISSN: 0193-4120 Page No. 4724 - 4727

hole Attack In Wireless Sensor network Using Trusting Mechanism	DR. NARENDRA M. SHEKOKAR2	Mechanism for Wireless Sensors		valuate the trust price of the node within the network that is just like the theory of trust in human society then this trust price is employed to notice the malicious activity in our case packet dropping
Detection or Removing the correct Black & Grey Hole Attack In MANETs	Sukla Banerjee	Mobile Ad-Hoc Networks (MANETs)	2008	Spite through all caution for entireinformations at single span a traffic separate the whole jams occures to some tiny size blogs. In order that malicious nodes is detected associated sepated in middle of the moving control of more such blocks by doing certain last thing on analysing at the nodes.
A Mechanism For Detection Of Grey Hole Attack In Mobile Ad Hoc Networks	JayedipSen, M. Giriish Chandra, Hariharan S.G.	Mobile Ad Hoc Networks (MANETs)	2007	The secured planning theory will raise the responsibility of finding the source by actively invoking a communicative and distributed rule which involving that the neighbour nodes will be a malicious grey hole node. That detects a call works on the rules of association supported by cryptography method of thresholds.

IV. PROBLEM DESCRIPTION

One of the foremost common attacks based on routing protocols currently a days-Grey hole and region attacks. To simulate a network with a malicious node (known as region and grey hole) on however the network functions beneath true of associate degree atack. In black-hole atack, once the

RREP msg is associated through supply node , is gained through the unwanted nodes, it generates a faux R-REP and leaves awfully massive worth in Destination line by line process forms variety field and singular cast it to the supply node. On getting this R-REP, the supply starts to forward information packets to unwanted node, presumptuous that it's having least and freshest path to the destination and ignores alternative RREP packets. The info packets received by malicious node don't seem to be forwarded by it to the other node. This attack is named Black-hole attack as a result of all the info packets square measure born by malicious node, the supply node Src needs to speak with destination Dest that it elaborated through the RREQ. However node a pair of and node five that is malicious nodes, single casts faux RREP to the supply, claiming that they recognize the small path to Dest whereas they are having no distance to Dest. Once supply intermediate to send information packet to them, the put together these packets. The region and grey hole attack can take away an outsized worth of impact to the performance of wireless mesh network. In multiple ways that the wrong characteristic could exhances by grey hole attack, grey hole attack could be a node that react unwanted for a some particular span of time length by catheartic packets however could come back to balanced behaviour and later forward the packets through packet ID to alternative packet. A

grey hole might also behave a random behaviour by that it rejects some the packets at random once it forward to alternative packets. Thereby its detection is even harder than region attack.

V. CONCLUSION

To get correct result in part attack, malicious node ought to position at the middle level of the wireless network. All these unwanted node generates wrongly developed R-REP infos as if it comes from other victing nodes rather than acquiring at its own, all messages are forwarded to the victim node. Grey hole attacks against one or 2 nodes within the network to isolate them, wherever as part attack affects the total network. Morely , the mallicious node that makes an attempt grey hole attacks can't be perceives simply since it doesn't send wrong messages. Behaviour of unsuccessful or full nodes could appear like inconsiderate nodes attacks or grey hole attacks because of dropping of messages. But, since unsuccessful nodes cannot stucked a replacement management message, they cannot type a part attack though they're going to drop the message later.

REFERENCE

[1] KannuGete, Piyoush Kumar Shukla, AnjanaJayantDeen," Grey Hole Attack in Wireless Mesh Networks - Survey", International Journal of Computer Applications (0975 – 8887) Volume 95– No.23, June 2014.

[2] N.Balaji, A.Shanmugam, "Dynamic Trust Based Method to Mitigate Grey hole Attack in Mobile Ad-Hoc Networks", International Conference on Communication Technology and System Design 2011, online at www.sciencedirect.com

[3] RupinterKaur, Parmender Sigh, "Black Hole and Grey hole Attack in Wireless Mesh Network", (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-3, www.ajear.org

[4] RubaliSharmma, "Gray-hole Attack in Mobile Ad hoc Networks: A Survey", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1457-1460

[5] Bansi S. Kantariya, Dr. Narendra M. Shekoka," Detection and Mitegation of Grey hole Attack in Wireless Sensors Network Using Trust Mechanism", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

[6] ChaudhariRajashri M, PatilManesh P, "Performance Evaluation of Attack Detection Algorithms in Delay Tolerant Networks", International Journal of Computer Applications (0975 – 8887) Volume 171 – No.4, August 2017

[7] Shaiffu, AmandeepKaurVirk, "Grey hole and Black hole Attack determining and Prevention using IP Backtracking in WSN", International Journal of Computer Applications (0975 – 8887) Volume 169 – No.5, July 2017

[8] GeetanjaliRathee and HemerajShaini, "A SECURE MANYCAST ROUTING PROTOCOL AGAINST GREY HOLE ATTACK", (ARPN) All rights reserved. VOL. 11, NO. 21, NOVEMBER 2016