Indian Journal of Science and Technology, Vol 9(22), DOI: 10.17485/ijst/2016/v9i22/90982, June 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Perception and Eradication of Energy Exhausting Attacks in WSN

M. Rajesh Khanna[1*], A. Rengarajan[2], R. Prabu[3] and S. Siva Shankar[4]

[1]Department of Computer Science and Engineering, St. Peter's University, Avadi, Chennai - 600054, Tamil Nadu, India; seenum84@gmail.com
[2]Department of Computer Science and Engineering, Vel Tech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai - 600062, Tamil Nadu, India; rengu_rajan@yahoo.co.in
[3]Department of Information Technology, Vel Tech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai - 600062, Tamil Nadu, India; dprpit@gmail.com
[4]Department of Computer Science and Engineering, ASET, Palakad - 678557, Kerala, India; sss_siva85@yahoo.co.in

Abstract

Microwaves ad-hoc feeler groups are spatially distributed self governing sensors to examine physical or environmental conditions and for conveyance purposes. Besides all the comforts of the life wireless network spouses serious security threats. Here we implement a simulation based model by using both dynamic threshold algorithm and recursive algorithm and hidden terminal process is used to transfer the data packets to the outer region nodes without any hazards. The proposed method detects the attack and restrain from the attacker node in the network based on CS (Cognitive Sensing) node.

Keywords: Cognitive Sensing, Dynamic Multicast Routing Protocol, Denial of Service, Hidden Terminal Communication Scheme, Recursive Algorithm, Wireless Sensor Network

1. Introduction

Wireless Sensor Networks (WSN) is advancing in the research field with new technologies in various application areas including environmental, medical, military crisis management, smart speech etc[1]. Due to its poor scalability and high communication overhead, it is naming to secure the data packets transferred through this network[2]. This security on the data being transferred can be ensured by implementing DORP, where the resident key file holds the decryption and encryption. However, it is challenging to secure the data packets efficiently because of the poor scalability and high communication overhead[3]. It identifies the type of vampire attacks. This causes the source node to send the packet to the malevolent node. Malevolent node resolve throw the respond RREP to the source node in the sense that it has the undeviating path to sink node[4]. This causes the nodes to reduce its battery power which leads to disable the network and also packet loss occurs[5].

We are concentrating on the Black fissure assault. It is a kind of denial-of-service assault in which a router that is hypothetical to relay data packets as a substitute rejects them.

Several examine works have been taken to solve the problem issues caused by malicious node in wireless adhoc sensor networks[6].

2. Proposed Converts the Random Nodes to Mesh Topology

Paper attempts to resolve this issue by implementing DORP, Hidden Terminal Communication process and Recursive Algorithm with Priority Mechanisms.

To avoid the collision and to prevent from the malicious node by using CS (Cognitive Sensing) node this has the information about the black hole nodes. Approach works efficiently in both static and dynamic stages of nodes. The basis node may not essential be able to identify which of the in-between nodes has the routing information to the

* Author for correspondence

target or malevolent node respond forged RREP. Lure address to persuade the malicious nodes and to utilize the reverse tracing programs to notice the accurate addresses of malevolent.

Initial Bait Step: A malevolent node to send a respond RREP by transfer entice RREQ to facilitate it has worn to advertise itself as having the unswerving path to the node that detains the packets converted. Source node stochastically selects adjacent nodes.

Preliminary overturn tracing stride: The overturn tracing plan is worn to identify the behaviors of malevolent nodes during the route respond to the RREQ message.

Shifted to imprudent guard Phase: Following the above primary proactive guard (steps A and B), the route detection is activated. As soon as the route is established and if at the end it is establish that the packet delivery ratio considerably cataract to the porch, the detection scheme would be trigger over to identify for unbroken maintenance and real-time reaction efficiency.

Random to Mesh:

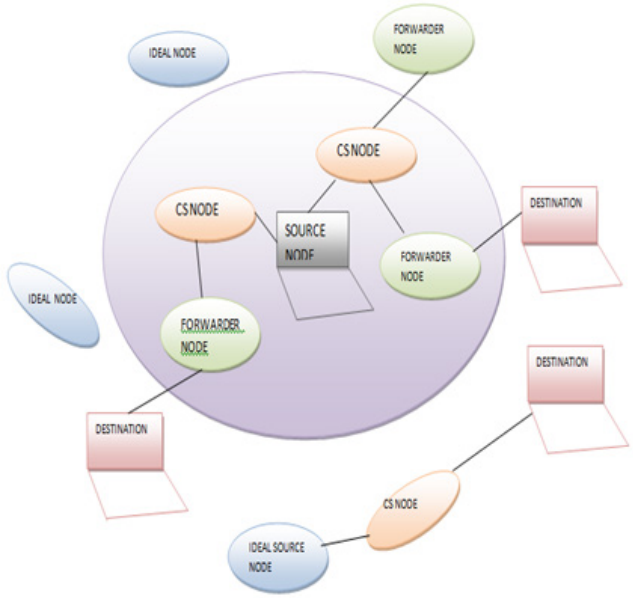

Figure 1. Architecture diagram.

Random to Mesh conversion is achieved by using DORP (Dynamic Multicast Routing Protocol). Mesh is formed among the basis and the target. To create the mesh each source sends the join req control packets periodically. The receiver upon reception of joinreq control packets from the source receiver can send joinrep through the reverse unswerving path. The joinrep packet contains basis id and correspondent after that node id. It sets a forwarding flag and becomes the forwarding node for the particular multicast group.

Past in the offing for a spiced time it invent a fresh joinrep packet and frontwards it. Intermediate node forwards the joinrep packet beside the overturn path to the basis establish the path. This protocol uses a malleable state move toward to uphold the mesh that is to restore the routes between the basis and recipient.

3. Experimental Evaluation

3.1 Recursive Algorithm

Supply nodes send the information packets to nearby CS node by using priority mechanisms in Recursive algorithm. Priority mechanisms classifies into two categories: Moment precedence mechanisms will manage the transmission sequences of buffered packets and gap precedence mechanisms control the access of buffer. Gap precedence mechanism categorized into Pushout and Partial buffer sharing mechanisms. In Pushout mechanisms the higher precedence packet may penetrate the queue even when it is full, by replacing the low priority packet already in queue. If a low priority packet arrives at the queue while it is full, it will be not needed. In Partial Buffer Sharing mechanisms both high and low priority packets are accepted by the queue until it reaches the porch. When this porch has been packed only high precedence packets will be acknowledged provide that queue is not full.

3.2 Dynamic Porch Algorithm

As soon as the route is established and stipulation at the destination it is originate that the packet Delivery proportion significantly falls to the threshold, the detection proposal would be triggered again to detect for unbroken maintenance. The dynamic porch algorithm reins the time when the packet delivery ratio cascade under the same threshold. If the sliding time is shortened, it earnings that the malicious nodes are still at hand in the network. In that case, the sill should be adjusted uphill.

If source node does not have any nearby CS node, in that case it will check he capability of nearby forwarder node that is whether it will have the capability of receiving the data packets that is transferred from the supply node or not. When node does not have the capability of receiving the data packets simply it forwards to the node which has controlled by the CS node. If the node has the capability of receiving the data packets it receives and forwards to destination.

3.3 Hidden Terminal Communication Scheme

Hidden nodes (node which are outside the mesh network) are nodes that are out of range of other nodes or a collection of nodes. The nodes manage transmission themselves by interrogating and yielding authorization to send and receive packets. This plan is frequently called RTS/CTS.

The fundamental idea is to confine the channel by notify other nodes about an upcoming transmission. This is done by invigorating the receiving node to outputting a petite frame so that in close proximity nodes can detect that a transmission is obtainable to take place. The closes by nodes are then expected to avoid transmitting for the duration of the imminent (large) data framework. This plan activates the ideal node which is beyond the mesh network. Therefore the packet delivery ratio is augment in wireless ad-hoc sensor network.

Experimental Result

NS2.35 Network simulator is worn to imitate a wireless network by way of DORP Protocol. The simulation results are given below:

3.4 Delay Analysis

Delay means that, moment taken to pass on the packets from starting place to target. Here we are comparing delay occurred in without using mesh networks and in mesh networks

3.5 Throughput Analysis

Throughput refers to the successful delivery of packets from source to sink. The existing system throughput of CBDS scheme is compared with proposed system including with HTCS.

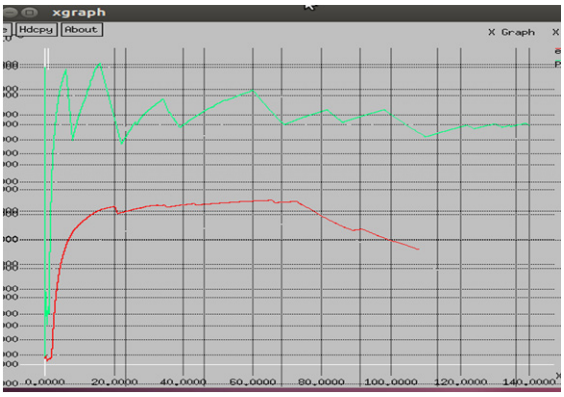

Figure 2. Delay analysis.

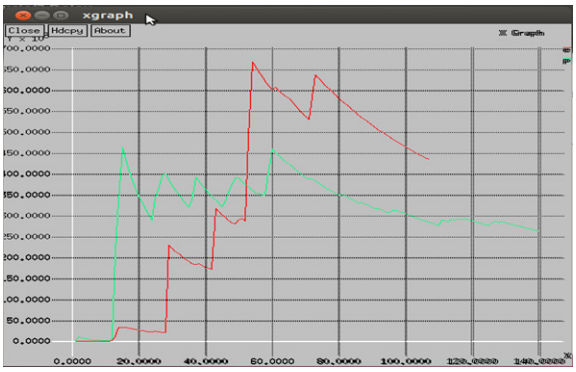

Figure 3. Throughput analysis.

4. Conclusion

We implemented a scheme called HTCS to activate the ideal nodes which are in outside the mesh network. Our proposed method detects the behavior of malicious node and provides the information to Cognitive sensing node. Thereby malevolent nodes are not used for communication of data packet from starting place to target.

The proposed method is compared with the previous bait method and the simulation results showed that our method increases the packet delivery ratio.

5. Acknowledgement

The authors gratefully acknowledge financial support from the Office of Orange.

6. References

1. Goyal P, Parmar V, Rishi R. MANET: Vulnerabilities, challenges, attacks, application. International Journal of Computational Engineering and Management. 2011 Jan; 11:32–7.
2. Revathi V, Pushpalatha M, Sornalakshmi K. Implementation of key exchange and secure routing mechanism in a wireless adhoc tesbeds. Indian Journal of Science and Technolgy. 2016 Mar; 9(10):1–9.
3. Ramya P, Gopalakrishanan V. An efficient timer based minimum path d-equivalance CDS construction for wireless adhoc networks. Indian Journal of Science and Technology. 2015 Apr; 8(S7):194–202.
4. Pagnis MS, Shrivastava AK. An efficient routing protocol for mobile ad-hoc network; 2013.
5. Chang JM, Tsou PC, Woungang I. Defending against collaborative attacks in mobile ad-hoc sensor networks; 2015 May.
6. Corson S, Macker J. RFC 2501, Mobile Ad Hoc Networking (MANET): Routing protocol performance