An Efficient Network Discovery Storage Based Resilient Packet-Forwarding Scheme for the Mitigation of Black Hole and Wormhole Attacks in 6lowpan Sensor Networks

B.Sudhakar, E.V.Abhinaya

Abstract: In wireless networks 6LOWPAN with the low power wireless devices has limited processing capabilities. In this network, the malicious node attacks at the network layer due to its nature of self configuration and dynamic network formation. It increased number of packet dropping attacks in network layer like Black Hole attacks and Worm Hole Attacks may cause the undesired operations in the time of routing the packet transfer. It degrades the performance of the legitimate users in the network. This work proposes an Efficient Network Discovery Storage Based Resilient Packet-Forwarding Scheme for the mitigation of malicious black hole and wormhole attacked nodes in 6Lowpan Sensor Networks. It also cooperates to manage the storage and prevent packet drop of sensor nodes present in the 6lowpan network.

Index Terms: Low Power and Lossy Networks (LLNs),Wireless Sensor Networks, (WSNs) Neighbor Watch System (NWS). Routing Protocol (RPL) ,6 (IPv6) Low Power over Wireless Personal Area Network (6LOWPAN)

I. INTRODUCTION

Low Power and Lossy Networks (LLNs) included with lot of embedded networking devices with fixed power, memory and processing resources. These devices are created by several of links and used in a various applications, including industrial monitoring, wireless sensor networks (WSNs), and smart grid automated metering infrastructures. The Internet of Things (IoT) provides guarded accessories in LLNs with Internet entrée. The on hand protocols in LLN are not applicable to focus the several communication patterns [1]. The major issue in WSN is lack of security because of their open and unattended deployment. Security mechanisms have been corrected Routing Protocol for LLNs (RPL)[2]. However, they can only protect the attack from external sources. So the RPL uncovered the wire range of security measure in terms of attacks.. In this proposed system, we focus the security attack referred as wormhole and black hole attack [3–5

Revised Manuscript Received on 30 July 2019.
* Correspondence Author

B.SUDHAKAR: Assistant Professor,Dept of ECE,Annamalai University Chidambaram-608002.

E.V.ABHINAYA:Dept of ECE,Annamalai University,Chidambaram-608002

This work focuses on the mitigation of malicious black hole and wormhole attacked nodes. This scheme also cooperates to manage the storage and prevent packet drop of sensor nodes present in the 6lowpan network protection. To mitigate effect of wormhole attack n in Low Power and Lossy6Lowpan sensor network, a distributed network discovery approach is used to determine whether wormhole attack is performing in the network or not.

For example some methods use statistical approach. They find sensational changes in the specific factual examples and after that choose presence of wormhole in the system. Longer proliferation can be another side effect of wormhole presence(6-10). Also we can decide the presence of wormhole in the system by checking the parameters, for example, greater transmission go than that of typical condition, and past hub isn't a neighbor too. The proposed strategy depends on the way that specified wormhole information originates from unapproved and illicit neighbors.

The 6Lowpan sensor networks causes the black hole attack by using Neighbor Watch System (NWS) over maliciously packet-dropping nodes. Here the proposed system implemented with single path data forwarding scheme for reducing power consumption. As the packet is sent along the single-way toward the base station, our plan, nonetheless, changes over into multipath information sending at the area where NWS distinguishes handing-off hubs' mischief. The watch hub can find and retransmit the packets when it is not transmitted(11-14).

It is vital that every hub communicates its neighbor's table and after that stores the neighbor's table of its neighbor’s, which devours more space for capacity. Also, the watch hubs need to store more bundles around them for potential retransmit, which requires vast support and more vitality utilization.

Here the sensor nodes are associate with each other to overcome the above problem through splitting of data. The major purpose of associate storage is to administer the accessible storage in the network to make sure the commitment of data collection for the longest possible without any disturbance. If the neighbor nodes are full then there is no possibility for data sharing.Thus the black hole and worm hole nodes are detected by frequent monitoring and relaying node’s misbehavior that are transmitted by the nodes and it will be removed from the network. Thus the framework results will be compared with the performance of the existing isolation techniques in simulation.

II. PROPOSED SCHEME

The Proposed scheme is used for the mitigation of malicious black hole and wormhole attacked nodes in 6Lowpan Sensor Networks. It also support to stop packet drop of sensor nodes present in the 6lowpan network.

In this work , the network discovery approach needs to mitigate its malicious node effect. The wormhole attack in 6Lowpan network is determined by checking the dramatic changes in the certain statistical patterns. It also uses Neighbor Watch System (NWS) against maliciously packet-dropping nodes in 6Lowpan sensor networks caused by black hole attacks. Neighbor Watch System detects relaying node's misbehavior This scheme consumes less power than multi-path schemes because it employs single-path data forwarding. This scheme employs multi-path data forwarding at the location to detect relaying node's misbehavior. The watch hubs need to store more bundles around them for potential retransmit. At the season of full hub's memory, it offloads its information to its neighbor hubs in capacity of free spaces and no reasonable neighbor hubs with adequate storage room, the sink is critically advised about the over-burden area that should be quickly dumped. This Scheme is included the accompanying three expressions

i) Network discovery
ii) Neighbor Watch System
iii) Storage Balancing

6Lowpan Network Discovery

The mitigate effect of wormhole attack in 6Lowpan related to wireless sensor network, a distributed neighbor discovery approach has been proposed. There are a few criteria to decide if wormhole assault is performing in the system or not. For instance a few techniques utilize measurable methodology. They find emotional changes in the specific factual examples and afterward choose presence of wormhole in the system. Longer engendering can be another side effect of wormhole presence. Furthermore we can decide the presence of wormhole in the system by checking the parameters, for example, greater transmission extend than that of ordinary condition, and past hub isn't a neighbor too. The proposed strategy depends on the way that specified wormhole information originates from unapproved and illicit neighbors. The issue of wormhole assault will be fathomed if the accepting hub can decide if entry information originates from genuine neighbor or not. Along these lines with the end goal to relieve the impact of aloof wormhole assault which aggressor isn't have a place with the system and does not utilize the sensor gadgets to get and forward the information through the wormhole burrow, neighbor revelation convention is utilized .

Neighbor Watch System

The proposed system looks to determine hop-by-hop believable delivery in face of maliciously packet-dropping nodes, basically employing single-path forwarding. In the way of delivering a single packet the proposed system works on multiple path diffusion forwarding. The existing system cannot provide the proper solution in terms of ACK based. With NWS, we can detect the packet delivery to the next hop nodes with its neighbor nodes shown in fig 2.1. The base methodology of our scheme is as follows:

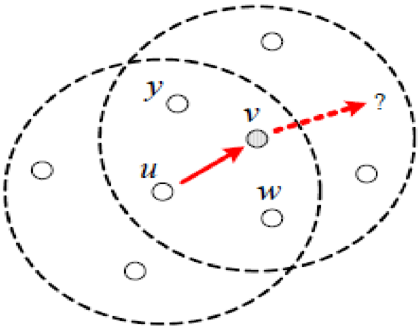


Fig 2.1 : Neighbor Watch System.

Storage Balancing

The 6Lowpan wireless sensor network included with set of moving sensors and a mobile node with unlimited resources that moves at a fixed speed around the field and gathers data on thefly. In the proposed system, the each and every node must communicate with neighbor's table and store the information on to the table. In addition, the watch hubs need to store more bunch around them for potential retransmit, which needs substantial support and more vitality utilization.

The proposed system make sure of their position, communication and storage gap. They watch occasionally the area of concentration, produce packets and buffer them close by while awaiting the arrival of the sink that moves in accidental mode to collect data.. In this approach a sink mobility for its skill to divide data load among all sensor nodes within the network and to make sure a high consistency in the data compilation process has been implemented and shown in fig 2.2.

While touching within the field, the mobile sink every so often broadcasts beacon messages to notify sensor nodes about its occurrence. Nodes having received the beacons upload their buffered data to the sink via one hop communication. At the time of full node's memory, it offloads its data to its neighbor nodes in function of free spaces and no suitable neighbor nodes with sufficient storage space, the sink is urgently notified about the overloaded region that needs to be rapidly dumped shown in fig 2.3.

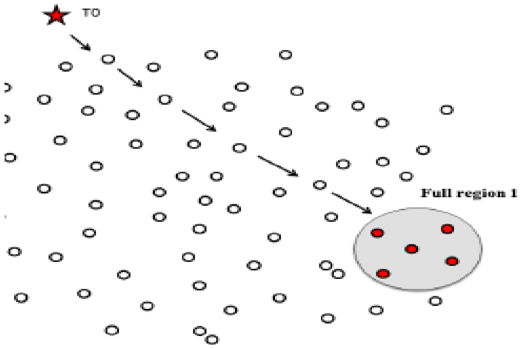


Fig 2.2 : The sink moves toward full region to offload data

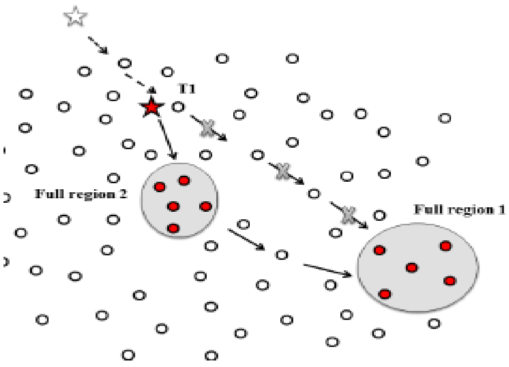
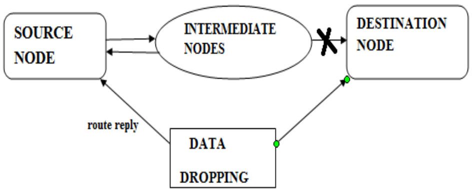


Fig 2.3 : The sink receives another request from region

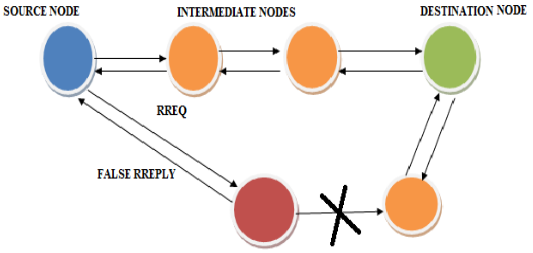
III. DIFFERENT TYPES OF ATTACKS

Black Hole Attack

It is more effective attack of DoS (Denial of Service). Black hole attack sends the reply route message as a shortest path to the source to reach the destination. Here, the data packets reach the destination with malicious node. The black hole attack is request reply method that provides reply as route reply and request as route request. It gives route request to its neighboring nodes and the malicious node provides route reply fallaciously as that of shortest path. The malicious node will drop all the packet data by providing route reply. Flow diagram of black hole attack and the architecture of black hole attack is shown in fig 3.1 and fig 3.2.



3.1.Flow Diagram of Black Hole Attack

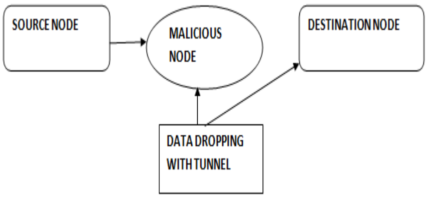


3.2. Architecture of Black Hole Attack

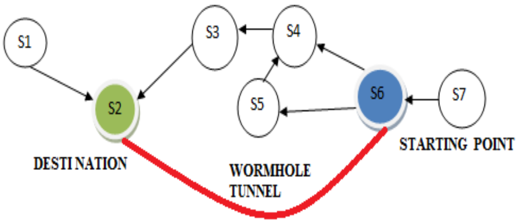
Here, the black hole attack gives request to its neighboring or intermediate node and the malicious node give back reply to the source node to drop the data packets. So the data packet does not reach properly to its destination node because of the malicious route reply.

Wormhole attack

It is a relay-based attack that can confuse the routing protocol for an unclear route to reach destination. It is very short node than the original node that can confuse the routing mechanism. It has more than one malicious node and tunnel between them, tunnel is covered with wire. The wormhole attacking node receives the packet data at one node and transmits that to another location so that destroys the desired route to the destination.



3.3.Flow Diagram of Wormhole Attack

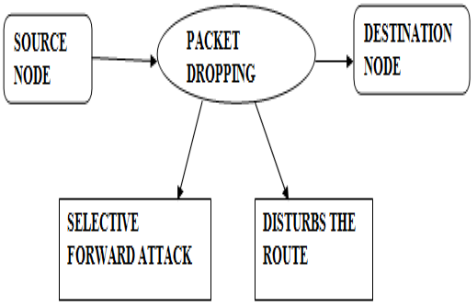


3.4 Architecture of Wormhole Attack

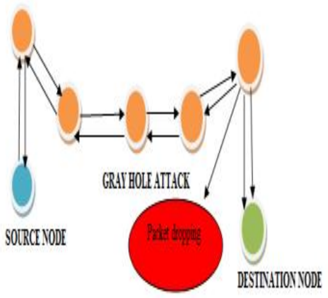
Flow diagram of Wormhole attack and the architecture of Wormhole attack is shown in fig 3.3 and fig 3.4.From this, the worm hole attack drops the data packets by using the wired tunnel. It confuses the routing protocol to drop the data packet. Here the worm hole attacks the nodes with more than one malicious attack.

Grayhole attack

It is a selective forward attack that creates a serious threat in terms of attacking data packets. Gray hole attack is a variation of black hole attack and it drops the data packet selectively. It has two phases, one is the malicious node selects the path itself to attack the data packet; another one is disturbs the route to drop the data packet. Gray hole follows the probabilistic distribution to select the route for dropping the data packet.



3.5 Flow Diagram of Gray Hole Attack



3.6.Architecture of Gray Hole Attack

Flow diagram of Gray hole attack and the architecture of Gray hole attack is shown in fig 3.5 and fig 3.6.Here, the gray hole drops the data packets selectively taken. It drops the data packet in two ways that, first the malicious node selects the route to drop the data packet and then it confuse the data packets in desired route.

IV. SIMULATION RESULTS

The simulation experiments has been taken using the NS2 to examine the performance of the novel approach. In this work, the performance has been measured in terms of detection rate, packet delivery ratio (PDR), Isolation Latency and energy consumption by changing key simulation parameters, including evaluation window (ω), packet drop rate, and the number of malicious nodes. For performance comparison, the proposed scheme had been compared against the standard existing RPL routing protocol .Hence the figures 4.1,4.2,4.3 and 4.4 shows that the proposed method has achieve the better performance than the existing method.

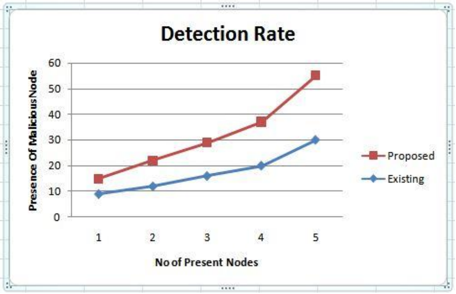


Fig 4.1: Detection Rate

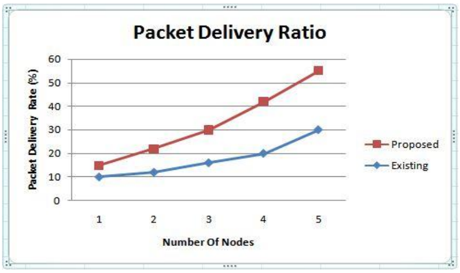


Fig 4.2: Packet Delivery ratio

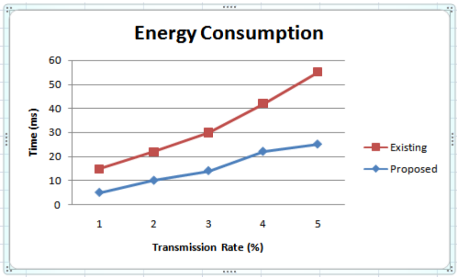


Fig 4.3 : Energy Consumption

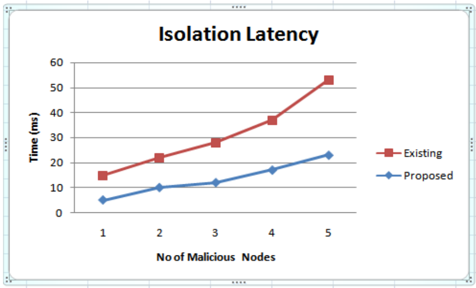


Fig 4.4 : Isolation Latency

V. CONCLUSION

The proposed system is mainly implemented for eliminate the malignant of black hole and wormhole attack in 6Lowpan Sensor Networks. This system also work together to administer storage and prevention of packet dropping in 6Lowpan Sensor Networks. The network discovery system is used to find existence of wormhole in the network by finding the wide changes in the certain statistical patterns. Neighbor Watch System (NWS) is used over malignant packet-dropping nodes in sensor networks caused by black hole attacks. This system implements multi-path data forwarding at the location to detect relaying node's misbehavior. The watch nodes need to store more packets around them for potential retransmit. Thus the black hole and worm hole nodes are detected by frequent monitoring and relaying node's misbehavior that are transmitted by the nodes and it will be removed from the network. Thus the framework results were compared with the performance of the existing techniques. Thus the simulation results shows that the proposed technique has better performance than the existing one.

REFERENCES

1. Chugh.K, Lasebae.A and J Loo, "*Case Study of a Black Hole Attack on 6LoWPAN-RPL*", Securware 2012: The 6th Intl. Conf. on Emerging Security Information, Systems and Technologies, UK, 2012.
2. Cheng, H., Yang, S., and Cao, J, Dynamic genetic algorithms for the dynamic load balanced clustering problem in mobile ad hoc networks, Expert Systems with Applications, Vol. 40, No. 4, pp. 1381-1392,2013.
3. Chunnu L and A Shrivastava, "*An Energy Preserving Detection Mechanism for Black Hole Attack in Wireless Sensor Networks*", Intl. Journal of Computer Applications Vo.115, No.16, April 2015.
4. Shivwanshi.O, Patel.R and Saxena.P, "*Cluster Based Secure WSN against the Balckhole and Grayhole Attack*", Intl. Journal of Computer Science and Information Technologies, Vol.6, No.6, pp.5470-5472,2015.

5. Kalaiselvan.K and Gurpreet Singh, "*Detection and Isolation of Black Hole Attacks in Wireless Sensor Networks*", International Journal of Innovative Research in Science, Engineering and Technology, Vol.4, No.5, May 2015
6. D Nitnaware and A Thakur, "*Black Hole Attack Detection and Prevention Strategy in DYMO for MANET*", 3rd Intl., Conf. on Signale Processing and Integrated Networks",2016.
7. Luis M.L. Oliveria, Joel.J.P.C Rodrigues, AmaroF.Sousa and Victor M.Denisov, "*Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms*", IEEE Trans. on Industrial Informatics, Vol.12, No.6, December 2016.
8. YueQie and Maode Ma, "*A Mutual Authenticaticaton and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks*", IEEE Trans. on Industrial Informatics, Vol.12, No.6, Decemeber 2016.
9. Ahmed and Young-BaeKo, "*Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks*", Article in Research Gate, October 2016.
10. Sudhakar B., Bensraj R, Performance Analysis of Text To Speech Synthesis System Using Hmm and Prosody Features With Parsing for Tamil Language, International Research Journal of Engineering and Technology, Vol. 03, No. 6, pp. 2233-2241,2016.
11. Deny, Sivaneshkumar, Sundarajan.M and .Khanna.V, "*Defensive against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach*", Intl. Conf. on Algorithms and Applications in Emerging Technologies, December 2017.
12. Sujatha.R, Srivaramangai.P, "*Enhancing security in Manets Communication Issues and Mechanisms*", International Journal of Computer Techniques – Vol. 4 – Issues 3 (79 - 83), 2017.
13. Sujatha.R "*Layer Attack Detection And Isolation Techniques in Manet*" International Journal Of Modern Engineering Research (IJMER), vol. 07, No.12 , pp. 01 – 04,2017.
14. Nalini Subramanian, Andrews Jeyaraj , Recent security challenges Computers & Electrical Engineering, vol.7,No.1,pp.28-42,2018.

AUTHORS PROFILE

B.Sudhakar received B.E in Electronics and Communication Engineering from Adhiparasakthi Engineering College, Melmaruvathur, Tamilnadu during 1996-2000. Then M.E from Annamalai University, Chidambaram during 2000-2002. After that started my carrier as Assistant Professor in Annamalai University. I have finished my Ph.D from Annamalai University by 2017. I have published my articles in various International Journals and Conferences.

Mrs.Abhinaya.E.V is a research scholar persuing her research in wireless communications from Annamalai University. she has done her masters in communication systems from Anna University and has published her papers in International journals. She has also attended some national and international conferences and various workshops to enhance her knowledge. Her area of interest includes sensor networks, wireless communication, Intrusion detections and threat control.