An Effective Mitigation of Various Attacks in 6lowpan Wireless Sensor Networks

M. Selvakumar

Assistant Professor of ECE
Department of Electronics and Communication Engineering,
Faculty of Engineering and Technology,
Annamalai University, Annamalainagar, Tamilnadu, India.
Email: ms.lecturer@gmail.com

***Abstract*: In recent years wireless sensor networks plays an important role in all types of communications in the world. To establish these networks Internet Protocol version 6 (IPv6) Low Power over Wireless Personal Area Network will play the vital roll... 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, Gray hole attack and Worm Hole attacks may cause the undesired operations in the time of routing the packet transfer. It affects the progress of the rightful users in the network. It proposed to eliminate the various attacks and improve the efficiency of the system.**

Index Terms: Low Power over Wireless Personal Area Network (LOWPAN, Wireless Sensor Networks (WSNs) Routing Protocol (RPL).

I. INTRODUCTION

Routing Protocol is designed for Low Power and Lossy Networks (RPL) to support communication among thousands of devices. Internet of Things (IoT) comprised of smart devices like sensors and actuators using RPL protocol. RPL is applied over different applications as industries, smart environments and urban areas. In this paper, a review on security attacks in wireless sensor networks is presented [1, 2]. Several research works have been undergone for resolving vulnerable security threats. Due to the increase in millions and billions of connected devices all over the world, security is a major issue. Hence the deployment of IoT sensor devices in Wireless Sensor Network (WSN) involves mechanisms and algorithms for providing confidentiality, privacy, authentication, attack identification and prevention. Hereby this paper work projects out the major requirements of security in WSN Since the participation of different attacks have been tremendously increased. RPL in IoT is enabled for many real-time applications which also include sensitive data transmissions.

Developments in recent technologies have more importance to use internet in human's day-to-day life. Worldwide usage of IoT deals some challenges and limitations to be overwhelmed. The traditional fundamentals used in IoT are IPv4, IPv6, WSN, IEEE 802.15.4, RPL and Low Power Wireless Personal Area Network (6LoWPAN). IoT is comprised of different objects as vehicles, buildings, smart devices, etc. Smart devices include mobiles phones and different types of sensors [3, 4]. Sensor devices in WSN is deployed for data acquisition, collection and analyzing. WSN with IoT covers several application of monitoring that are in industries, human health, electrical equipment, natural disaster, city pollution, water quality, smart grid, smart home, intelligent transportation ,etc,. The growth of IoT is also applicable for Radio Frequency Identification (RFID) and mobile communications. IoT is comprised of four significant layers as sensing layer, network layer, service layer and interface layer.

RPL supports various applications in recent trends, RPL uses IPv6 based on distance-vector proactive routing protocol. Traditional process followed in RPL is the construction of Destination-Oriented Directed Acyclic Graph (DODAG) in the network. To build DODAG four significant control messages are used such as DODAG Information Solicitation (DIS), DODAG Information Object (DIO), Destination Advertisement Object Internet of Things use RPL Smart Home Smart City Smart Parking Online Shopping Agriculture [5, 6].
This work proposed on the mitigation of various attacks in various 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 towards the base station, our plan changes over into multipath information sending at the area where distinguishes handing-off hubs' mischief. The watch hub can find and retransmit the packets when it is not transmitted.
.

II. PROPOSED SCHEME

The Proposed scheme is used for the mitigation of various attacks such as black hole, Gray hole attack **and** wormhole attacked nodes in 6Lowpan Sensor Networks. It also cooperate to manage the storage and prevent 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 Two expressions

i) Neighbor Watch System
ii) Storage Balancing

(i) 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 [7, 8]. With NWS, we can detect the packet delivery to the next hop nodes with its neighbor nodes shown in fig 1. The base methodology of our scheme is as follows:

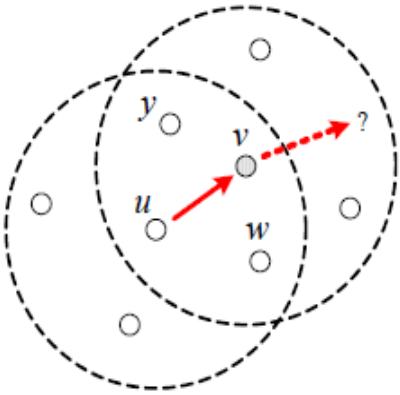

Fig 1: Neighbor Watch System.

(ii) 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 the fly. 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 [9]. 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.

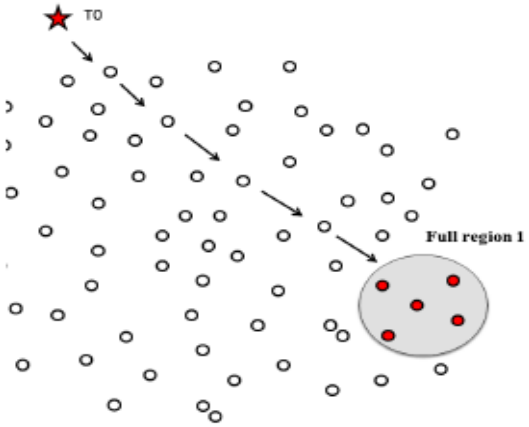

Fig 2: The sink moves toward full region to offload data

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 3.

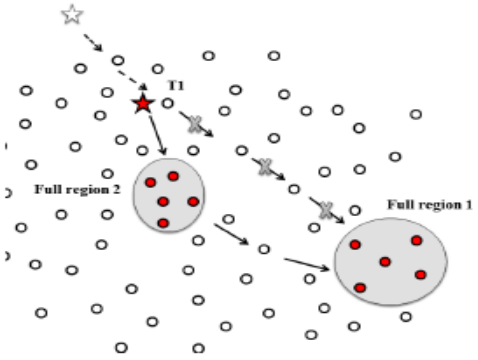

Fig.3: The sink receives another request from region

III. DIFFERENT TYPES OF ATTACKS

Common Attacks against RPL

In RPL attacks are generally classified into three categories as resource based, topology based and traffic based. Each category of attack is sub classified into two other partitions. The major classification of attacks that occur in RPL routing. Resource based RPL attack is further classified into direct and indirect attacks. Traffic plays a major role in RPL due to the increased number of user's participation, therefore attackers penetrate the network via traffic. Traffic based attacks in RPL are classified into Eavesdropping and misappropriation. The Eavesdropping attackers perform malicious activities as listening to other packet transmission and extracting the routing information from packets. The third category is network topology based attacks which is sub classified into sub-optimization attacks and isolation attacks. The goal of the attackers in sub-optimization attack is to minimize the performance of the entire network by involving into optimal path selection process. These thinks has to be eliminated by efficient discovery system

Black Hole Attack

The black hole attack 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 [10]. 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.
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.

Worm Hole attack

Wormhole attack 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 [11]. 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.

Gray Hole attack

Gray hole attack 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 [12]. 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 result has been achieved using the NS2 to inspect the performance of the novel approach. In this work, the performance has been calculated in terms of packet delivery ratio (PDR), and energy consumption by changing key simulation parameters, including packet drop rate, and the number of malicious nodes. For performance comparison, the proposed scheme has been compared against the standard existing RPL routing protocol .Hence the figures 4 and 5 shows that the proposed method has achieve the better performance than the existing method.

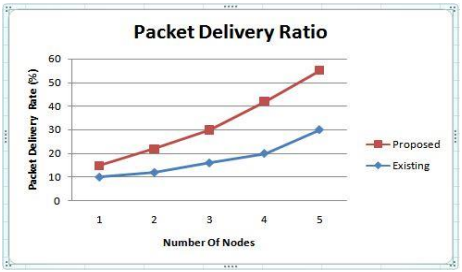

Fig 4: Packet Delivery ratio

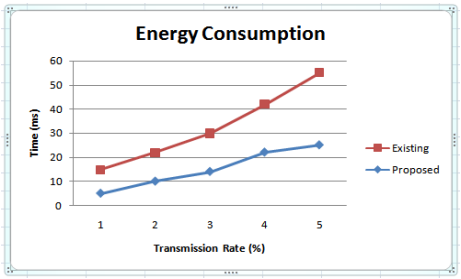

Fig 5: Energy Consumption

V. CONCLUSION

The proposed system is mostly simulated for discard the malignant of black hole, Gray 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. 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 previous system.

REFERENCES

[1] 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.

[2] 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.

[3] Ming Zhao, Arun Kumar, Peter Han Joo Chong, Rongxing Lu, "A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities", Peer-to-Peer Networking and Applications, Springer, vol. 10, no. 5, pp 1232 – 1256, 2017.

[4] Deepak Sharma, Ajay Narayan Shukla, "A Comparative Study of the Routing Protocols LOAD and RPL in Low and Lossy Networks (LLN)", Journal of Engineering and Technology, vol. 2, no. 1, pp 85 – 87, 2014.

[5] George Oikonomou, Iain Phillips, Theo Tryfonas, "IPv6 Multicast Forwarding in RPL-Based Wireless Sensor Networks", Wireless Personal Communication, Springer, 2013.

[6] Anhtuan Le, Jonathan Loo, Yuan Luo, AboubakerLasebae, "Specification-based IDS for securing RPL from topology attacks", IEEE IFIP Wireless Days, 2011.

[7] Sujatha.R, Srivaramangai.P, ”Enhancing security in Manets Communication Issues and Mechanisms”, International Journal of Computer Techniques – Vol. 4 – Issues 3 (79 - 83), 2017.

[8] Ahmed and Young-BaeKo, “Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks”, Article in Research Gate, October 2016.

[9] YogitaPundir, Nancy Sharma, Yaduvir Singh, “Internet of Things (IoT): Challenges and Future Directions”, International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, no. 3, pp 960 – 964, 2016.