Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 423 – 430

Procedia Computer Science

International Conference on Information Security &Privacy (ICISP 2015)11-12 December 2015 Nagpur, INDIA

Optimal Cluster Head Selection Based Energy Efficient Technique for Defending against Gray Hole and Black Hole Attacks in Wireless Sensor Networks

Snehal P. Dongare[a] , Prof. R. S. Mangrulkar[b]

[a]M.Tech. (Computer Science and Engineering),Department of Computer Engineering ,B. D. College of Engineering,Sevagram-442102, WARDHA (M.S.) INDIA
[a]snehal.dongre@gmail.com
[b]Associate Professor and Head,Department of Computer EngineeringB. D. College of Engineering, Sevagram-442102, WARDHA (M.S.) INDIA,
[b]rsmangrulkar@gmail.com

Abstract

Wireless Sensor Networks (WSNs), is prone to various types of attacks and security threats. Due to its dynamic topology, highly decentralized infrastructure and resource constraint sensors, proper energy utilization becomes a challenging issue. Such entities are responsible to make WSNs susceptible to various types of denials of service attacks which results in disastrous consequences like energy-hole creation in the network. Various cluster head selection based energy efficient protocols have been proposed to improve the lifetime of WSNs. In most of the energy efficient techniques, different approaches for energy utilization by sensors are proposed to extend lifetime of WSNs. The earlier scheme is defend against cooperative Gray-Hole and Black-Hole attacks that lead to performance degradation in WSNs containing mobile sensors. In order to overcome this, an energy efficient technique is presented in this paper to mitigate the impact of both kind of attacks simultaneously, on improving cluster head selection mechanism. Here, an energy efficient technique, on detecting and preventing compromised node to be a part on network communication in WSNs. The honest nodes is also determined to entrust as cluster head during packets transmission phase. The simulation results compare proposed protocol with state of the art LEACH protocol, which argues that the proposed scheme effectively minimize the chance of compromised node to become the cluster head and significantly improves network performance using networks dynamics viz. Packet Delivery Ratio(PDR), throughput , end-to-end delay and energy utilization in WSNs.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords:Black-Hole Attack; Cluster Head Selection; Energy Efficiency; Gray-Hole Attack; LEACH; Network Delay; Network Lifetime; Packet Delivery Ratio; Throughput ;Wireless Sensor Networks.

1. INTRODUCTION

Wireless Sensor Network (WSN), is a distributed system consists of Base Stations (BS) and large number of mobile Sensor Nodes (SN) that integrate micro sensing, computing and wireless communication capabilities, which are capable of detecting various events related to its surrounding environment such as speed, temperature, pressure, difference in displacement, light, etc. This paper proposes multi-hop inter-clustering protocol that selects most optimal Cluster Head (CH) with maximum residual energy at each round of CH selection mechanism along with preventing compromised node to become CH, which leads to better performance than LEACH. The rest of the paper is organized as follows. Section II provides an overview of the original LEACH protocol. Section III explains the security constraints in WSNs introducing Gray-Hole and Black-Hole attacks, whereas other previous enhancements of LEACH related to mentioned attacks along with their performances are discussed in section IV. Section V focus on implemented work where detecting attacks and its impact on WSNs has been elaborated. The conclusion and future direction for further work is presented in section VI.

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.084

2. LEACH PROTOCOL

LEACH (Low Energy Adaptive Clustering Hierarchy) is a common clustering algorithm that allows dynamic selection of cluster heads for distributing energy utilization among all of the sensor nodes in WSNs. LEACH is divided into number of rounds for selecting cluster heads. LEACH uses one hop inter-clustering to reach the faraway BS which misses the cooperation among cluster heads which is a major drawback of LEACH as more energy is consumed by the sensor nodes that are far away from the BS. Multi-hop inter-clustering algorithm leads to better performance in terms of energy conservation that leads to increase in lifetime of WSNs. At the beginning of each round of CH selection normal node chooses a random number x between 0 to 1 and checks if it is less than a certain threshold value T (n)[20],then it is converted from normal node to CH node, where the threshold function is defined as follows:

$$T(n) = \begin{cases} \frac{P}{1-P*\left(r mod\left(\frac{1}{P}\right)\right)}, n \epsilon G \\ 0, \quad otherwise \end{cases} \quad (1)$$

where P is the desired percentage of CH which is a predefined value (e.g. P=0.01), r is the current round number, and G is the set of nodes in the last 1/p rounds, that has not been selected as CHs. The main purpose to design and develop an energy efficient technique for WSNs is to improve the network lifetime and to increase the overall performance of network. In order to achieve this goal, many energy efficient techniques are available based on different parameters viz. , to improve CH selection approach, to reduce energy consumption of individual nodes, on improving inter cluster communication mechanism along with an optimal technique of cluster formation, residual energy based approach ,on calculating threshold value to select optimal set of CHs on considering various network topological parameters like average distance between sensor nodes and BS, area of the field and number of sensor nodes deployed over field.LEACH is better than conventional routing protocols as the responsibility of CH is distributed around all the sensor nodes, and also data aggregation by CH from member nodes reduces energy dissipation of the network. But LEACH still ignores the residual energy at each node during the CH selection stage and also the impact of malicious attacks encounter in the WSNs. This ignorance motivates to work on this challenging issue.

3. SECURITY CONSTRAINTS IN WSNS

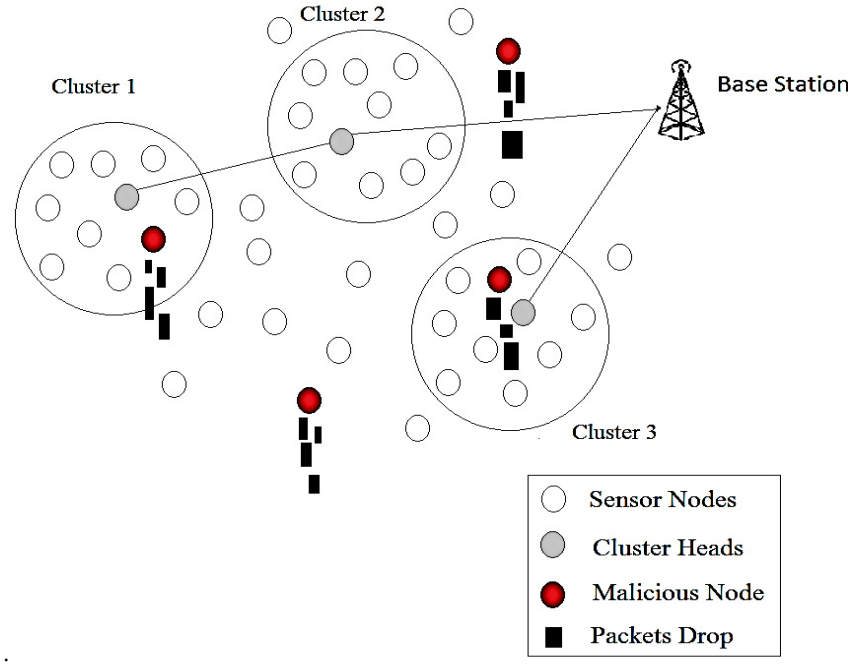

Figure 1. Design Overview of Attacks in WSNs

WSNs encounters number of security threaten attacks .A Gray-Hole (Packet Drop) attack or Black-Hole (False Report) attack is a type of denial-of-service attack accomplished by dropping packets. The attack can be accomplished either selectively by dropping packets for a particular specified network destination, a packet drops for every *n* packets or for every *t* seconds, or for randomly selected portion of packets, which is called Gray-Hole attack or in bulk, by dropping all packets. A malicious node may falsely