Discover and Prevent the Sinkhole Attacks in Wireless Sensor Network using Clustering Protocol

[I]Vishwas D B, [II]Chinnaswamy C.N, [III]Dr.T.H.Sreenivas
[I]PG Student, CNE, [II]Associate Professor, [III]Professor
[I,II,III]Dept. of IS&E, The National Institute of Engineering, Mysore, India

Abstract

Wireless sensor network (WSN) is one of the new network techniques and it consists of any small wireless sensor nodes. These nodes are capable of sensing and send data to base stations. Sinkhole attacks are work by making a compromised node look especially attracts network traffic by advertising fake routing updates. This fake updates are creates opportunities for attackers. So we want to detect and avoid sinkhole attack, many different methods are used to detect and avoid sinkhole attacks.

I propose a method to detect and avoid the sinkhole attacks for clustering technology in wireless sensor networks. Initially network is divided into number of clusters, every cluster has one header and the header is directly communicated to destination. In HEED clustering protocol the header nodes are not selected randomly. We examine our work in terms of throughput, packet loss rate, and end to end delay.

Keywords

Sinkhole, Clustering protocol, HEED, Aggregation, Mobile Agent.

I. Introduction

Wireless sensor network (WSN) is a system of network spatially distributed devices using wireless sensor nodes to sense environmental or physical conditions.

The Individual nodes are competent of sensing their environments and sending data to one or more compilation

Points in a WSN. One of the most significant issues for WSNs is efficient data transmission.

A. Sinkhole attack

Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the fake routing algorithm. Sinkhole attack attempts to harm WSN's where in an intruder attempts to redirect all network traffic towards itself, by providing falls routing data. These effects on the network load balance as well as it provide sausage for other attacks.

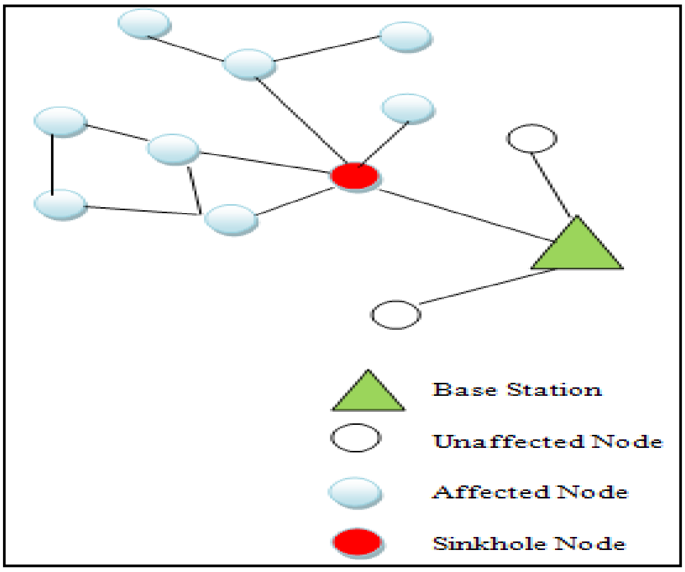

Fig 1.Example of sinkhole attack in wireless sensor network.

B. Clustering technology

Clustering divides nodes into groups which are called clusters. Each cluster is managed by a cluster head and all members are coordinated with the cluster head. Cluster heads are responsible for communicating with their own members and other cluster heads. There are diverse methods for selecting cluster head. In some methods cluster head is selected by cluster members; while, in other methods cluster head is selected by network designer. Cluster head may either remain constant during network lifetime or change based on the algorithm. The same is true for members of clusters. In clustering methods each sensor is either a cluster head which introduces itself in a specific region or is a member which must introduce itself to cluster head and become its member. The members are only able to communicate with their own cluster head and transmit.

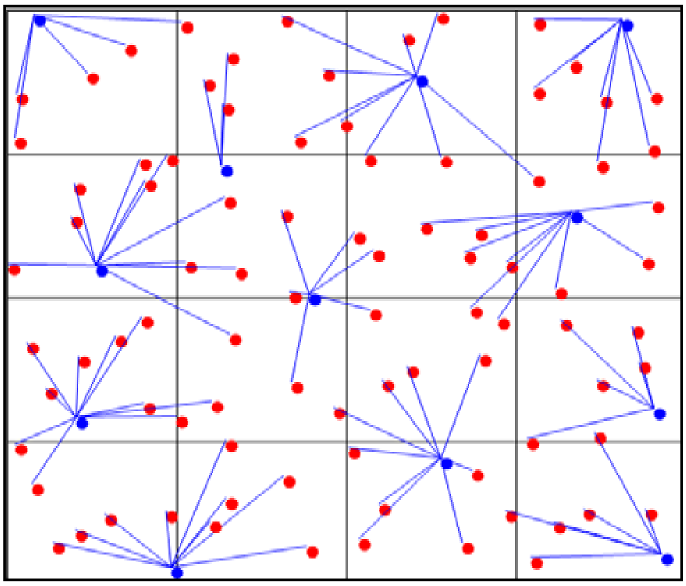

Fig 2. Clustered wireless network.

II. Existing System

In existing system the mobile agent technology based security solution against sinkhole attack for wireless sensor networks (WSNs). WSN has a dynamic topology, intermittent connectivity, and resource constrained device nodes.

Mobile agent is a program segment which is self-controlling. They navigate from node to node not only transmitting data but also doing computation. They are effective paradigm for distributed

applications, and especially attractive in a dynamic network environment. This mechanism does not require more energy
Sinkhole attacks are work by making a compromised node look especially attracts network traffic by advertising fake routing updates. This fake updates are creates opportunities for attackers. So we want to detect and avoid sinkhole attack, many different methods are used to detect and avoid sinkhole attacks.

1. Existing Approaches

Different peoples are proposed different methods to detect and avoid sinkhole attacks .here we discusses these methods.

We consider some previous researchers papers they may be classified into rule based, anomaly based, statistical methods, hybrid systems, cryptographic key management.etc

Rule based: In this approach rules are designed based on the technique or behaviour used to launch attacks (sinkhole attacks). These rules are running on each sensor node. Any node will be considered an isolated and adversary from the sensor network if it attacks the rules.

Anomaly based: In this method detection and avoid using search the anomalous in the network. Subset of anomaly based detection approaches are Rule based and statistical approaches.

Statistical: In this approaches we recorded data associated with some activities of the sensor nodes in network. Then the compromised node is detected by using comparing the correct behaviour of the threshold value the values are used as reference, any seniors node are above that threshold value is considered that nodes are an intruders .

Cryptographic: In cryptographic approach the dates are protected by using encryption and decryption keys for integrity and authenticity of packets travelling in the whole network. If packets are transmitted in consider network is encrypted the information such that to access the information we requires a key and we can alter the information can be easily detected.

Hybrid: In hybrid method we combine both the combination of both cryptographic approaches and anomaly approach. Benefits of this approach are can able to catch malicious nodes when their signature is not included in detection database and we reduced the false positive rate by using combination of both approaches.

III. Proposed System

In proposed system I focus on clustering and sinkhole attacks. Here instead of mobile agent broadcasting technique.

We use HEED Cluster concept and broadcasting of messages done through the cluster heads.

Clustering is an effective and convenient way to enhance performance of the WSNs system. Efficient data transmission is one of the most important issues for WSNs. Initially network is separated into number of clusters, each cluster is headed by a cluster header and the header is directly connected to destination. The header upon identifying the detecting nodes selects a set of nodes randomly and broadcast a unique value to their authentication keys, to the selected set of nodes in first round of data aggregation.

When any node within the group needs to transfer the data, it transfers slices of data to other nodes in that group, encrypted by individual authentication keys. Each receiving node decrypts, sums up the slices and transfers the encrypted data to the cluster header. The header aggregates and encrypts the data with the shared secret key of the destination and forwards it to the destination. The set of nodes is reselected with new set of authentication keys in the second round of aggregation.

When monitoring cluster-heads, member nodes of a cluster-head take turns to monitor this cluster-head. This mechanism reduces the monitor time, and therefore saves the energy of the member nodes. When monitoring member nodes, cluster-heads have the authority to detect and revoke the malicious member nodes clustering is an effective and convenient way to enhance performance of the WSNs system.

For clustering we used HEED protocol this protocol is a hierarchical, distributed, clustering scheme in which a single-hop communication pattern is retained within each cluster, where as multi-hop communication is allowed among CHs and the BS. Only sensors that have a high residual energy are expected to become CH nodes and broadcast a unique value to their authentication keys, to the selected set of nodes in first round of data aggregation. Any node needs to transfer the data within the group, it transfers slices of data to another nodes in that group, encrypted by individual authentication keys and in receiving end decrypts then combine the slices finally transfers the secure data to its cluster header .The cluster header aggregates and encrypts the data with the shared secret key of the destination and forwards it to the destination. using clustering technique along with replicated mobile agents to prevent the wireless sensor network from sinkhole attacks. and use mobile agents to aware every node from its trusted neighbouring nodes so they do not listen to the traffics generated by malicious nodes. We are using clustering technique along with replicated mobile agents to prevent the wireless sensor network from sinkhole attacks and use mobile agents to aware every node from its trusted neighbouring nodes so they do not listen to the traffics generated by malicious nodes. We examine our work in terms of throughput, packet loss rate, and end to end delay.

Slice method: - When a node wants to send data to its neighbouring nodes, it slices the data into number of pieces (since network size is depends on pieces). It holds the one of the slices with it. The remaining slices are encrypted with their respective authentication keys and sent to rest of the nodes.

IV. Literature Survey

Md. Ibrahim Abdullah et. al. [1] presented a technique to successfully detect the sinkhole attack when this malicious node located at far distance from base station. The technique is also applicable to wormhole attack as the attack is almost similar to sinkhole attack. Proposed technique is also applicable when sinkhole nodes advertise high quality link, strong transmitted power etc. Here we have to sort the advertising parameter and take decision which value is strange.

In (P. Samundiswary and Dananjayan, 2010)[3] a secured path redundancy algorithm has been applied to implement in heterogeneous sensor networks by using alternate path scheme in these networks with mobile nodes for mobile sinks to defend against sinkhole attacks. This proposed approach is not suitable for homogenous sensor networks.

In (D Sheela[2] and Mahadevan, 2011) they introduced mobile agents to detect the sinkhole attack in wireless sensor networks. But in this as the number of nodes increases the overhead of the network also decreases that degrade performance of the network.

In (Sina Hamedheidari and Reza Rafeh, 2013) they provide a mobile agent based approach to detect and prevent the sinkhole attacks in wireless sensor networks. They used mobile agents to detect malicious nodes and trusted neighbours in order to inform nodes from their environment.

Bhoopathy, V[4] In this paper they propose a securing node capture attacks for hierarchical data aggregation in wireless sensor networks. Initially network is separated into number of clusters, each cluster is headed by an aggregator and the aggregators are directly connected to sink. When any node within the group needs to transfer the data, it transfers slices of data to other nodes in that group, encrypted by individual authentication keys. Each receiving node decrypts, sums up the slices and transfers the encrypted data to the aggregator By simulation results, we demonstrate that the proposed technique resolves the security threat of node capture attacks.

Haowen Chan et al [5] Secure hierarchical in-network data aggregation is guaranteed to identify any manipulation of the aggregate by the adversary beyond what is achievable through direct injection of data values at compromised nodes. In other words, the adversary can never gain any advantage from misrepresenting intermediate aggregation computations. The system incurs only O(Δlog2 n) node congestion, supports arbitrary tree-based aggregator topologies and retains its resistance against aggregation manipulation in the presence of arbitrary numbers of malicious nodes. The main algorithm is based on performing the SUM aggregation securely by first forcing the adversary to commit to its choice of intermediate aggregation results.

Sanjeev Kumar Gupta[6] In WSNs there is one mechanism used to enlarge the lifespan of network and provide more efficient functioning procedures that is clustering. Clustering is a process to subdivide the sensing field of sensor network into number of clusters. Each cluster selects a leader called cluster head. A cluster head may be elected by the sensor node in the cluster or pre assigned by the network designer. Optimized Clustering can save lot of energy in the network. In our paper we have surveyed various clustering protocols for wireless sensor networks and compared on various parameters like cluster count, cluster size, cluster density, message count, node deployment, heterogeneity of nodes, location awareness and cluster head selection process etc.

Radhikabaska et [6] proposed an intrusion detection system against sinkhole attack in wireless sensor networks with mobile sink. This scheme is based on a hierarchical topology to secure any cluster-based routing protocols. signature technique that represents the detection data rate of a we can hinder deploying a replicated false mobile sink .Cell leaders activate their IDS only when sinkhole event occurs. This permits to reduce the number of nodes running their IDS and minimize energy consumption.

V. Conclusion

The main aim is avoiding sinkhole attack in WSN, sinkhole attack means duplicate nodes confuse and attract the nodes of entire network and reduce the network performance .Therefore we have Securing Node Capture Attacks for hierarchical data aggregation .The aggregator aggregates and encrypts the data with the shared secret key of the sink and forwards it to the sink.

Saving the energy of the nodes and reduce time consuming of network by using HEED clustering protocol. In HEED clustering protocol the header nodes are not selected randomly and using clustering technique along with replicated mobile agents to prevent the wireless sensor network from sinkhole attacks. Mobile agents are software entities which can function autonomously in a particular environment. They are able to carry out some activities in a flexible and intelligent manner.

References

[1] *Md. Ibrahim Abdullah "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count" Computer Science and Engineering, Islamic University, Kushtia, Bangladesh*

[2] *D.Sheela Naveen kumar "A NON CRYPTOGRAPHIC METHOD OF SINK HOLE ATTACK DETECTION IN WIRELESS SENSOR NETWORKS" . Computer Science and Engg Computer Science India Bangalore, India*

[3] *Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao "Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks" NICTA Victoria Research Laboratory Department of Computer Science and Software Engineering The University of Melbourne, Australia*

[4] *Bhoopathy, V. "Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks" International Journal of Engineering Research and Applications (IJERA). Department of CSE, Annai Mathammal Sheela Engineering College, Tamil Nadu, India*

[5] *Haowen Chan et al "Secure Hierarchical In-Network Aggregation in Sensor Networks" Carnegie Mellon University*

[6] *Radhikabaskar, Dr.P.C.Kishore Raja, et al "Sinkhole Attack Detection In Hierarchical Sensor Networks" .IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 978-1-4577-0590-8/11/$26.00 ©2011 IEEE MIT, Anna University, Chennai. June 3-5, 2011*