ISSN: 0975-766X
CODEN: IJPTFI
Available Online through Research Article
www.ijptonline.com

ENERGY EFFICIENT TECHNIQUE FOR DETECTING ATTACKS IN WIRELESS SENSOR NETWORKS

Naga Durga Siva Kumar.G*, V.Niteesh, Kiran.K , P.C.Kishore Raja, Radhika Baskar
Department of ECE, Saveetha University.

Received on: 10.08.2016 *Accepted on: 06.09.2016*

Abstract

In general, wireless sensor networks possess a number of sensor nodes that are capable of sensing, computing and communicating. In order to perform all these functionalities, sensor node utilizes some amount of energy from its battery source. The main drawback of wireless sensor network is that each sensor node is energy limited. Thus it is necessary to make use of the available energy efficiently to perform the functions effectively. Also, wireless sensor networks with many-to-one communication are highly subjected to security threats. Among all kind of attacks existing, sink hole attack is the most destructive routing attack for these networks, where an intruder attracts surrounding nodes with unfaithful routing information, and then performs selective forwarding or alters the data passing through it.

Here, we present an efficient and trust based secure algorithm to detect the sinkhole attack in wireless sensor networks. In this, AODV protocol is used during the packet transmission phase and an algorithm is designed where it detects the sinkhole attacked node using hop count as the base parameter. The entire simulation is carried out in the NS-2 simulation software. We ended-up with the evaluation of accuracy of the proposed algorithm to detect sink hole attack in Wireless sensor network.

Key Words: Attack detection, Sinkhole Attack, Trust Based Algorithm, Energy Efficiency, Attacks in Wireless sensor networks, Secure algorithm.

I. Introduction

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN) [1] [2], are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

As a product of the development and combination of the sensor technology, embedded computer technology, wireless communication technology and distributed information processing technology, Wireless Sensor Networks (WSNs) provide a kind of brand-new information acquisition and processing method, and have broad application prospects in military, environmental protection, agriculture and health and other fields [3]. Wireless sensor networks (WSN's) (also called wireless sensor and actor network (WSAN)) are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure etc. and to cooperatively pass their data through the network to a main location. Thus, the Wireless sensor Network is built of nodes– from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each sensor in WSN communicates its information with the base station present in its network. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance: today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on [4].

In WSN's, Each sensor node can form a multi-hop self-organizing network through wireless communication, and each sensor node is capable of sensing, data processing and communication. Generally speaking, wireless sensor network is often deployed in an open environment, even the enemy-occupied domain. As sensor nodes transfer data through wireless communication link, the network can be easily captured and invaded. Due to the lack of foundation infrastructure like wired network, what wireless sensor networks face not only traditional security threats but also some attacks which include the exhaustion attack, selective forwarding-attack, wormhole-attack, collision attack, sinkhole-attack, Sybil attack, hello-flood-attack, etc… Besides, each sensor node has limited energy and processing capability, small storage capacity and low bandwidth, this put forwards a larger challenge for the security of wireless network.

Here, we are presenting an efficient and trust-based algorithm to detect the sinkhole attack present in the wireless sensor networks. Sink hole attack is the most destructive among other attacks present in wireless sensor network.Sinkhole attack is one of the severe attacks in wireless Ad hoc network. In sinkhole Attack, a compromised node or malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. After receiving whole network traffic it modifies the secret information, such as changes made to data packet or drops them to make the network complicated. A malicious node tries to attract the secure data from all neighbouring nodes. Sinkhole attacks affects the performance of Ad hoc networks protocols such as AODV by using flaws as maximizing the sequence number or minimizing the hop count [5]. In this way the path presented through the malicious node appears to be the best available route for the nodes to communicate. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify. We used AODV protocol to communicate with neighbouring nodes. When a node wishes to send a packet to some destination, it checks its routing table to determine if it has a current route to the destination. If yes, forwards the packet to next hop node. If No, it initiates a route discovery process. It begins with broadcasting of RREQ to its neighbours specified for certain destination. Once an intermediate node receives a RREQ, It checks its routing table for route to destination. If found send RREP to source. If not found it rebroadcast RREQ to its neighbour nodes by setting up a reverse route path to source node in its route table. It ignores RREQ if it is processed already [6]. Finally on reaching RREQ to destination node, It unicast RREP to source node by using reverse route to source node.

II. Objective

The main aim of our project is to design an efficient and trust based secure algorithm to detect the sinkhole attack in Wireless Sensor Networks.

As these wireless sensor networks functions with one-to-many communication technology, they are easily exposed to the attacks. Some of the attacks are very general and does not interrupt the system while attacking. Whereas the sinkhole attack shows its impact on the whole system by destroying the entire network. Thus it is regarded as the most disastrous attack of all others. Also the networks are provided with limited energy source. Hence it is much important to design a energy efficient and trust based algorithm to determine the most disastrous attack called sinkhole attack in Wireless Sensor Networks.

III. Methodology

In this paper, we used AODV protocol for the transmission of the packets between the nodes. An efficient algorithm is designed in order to find the sink hole attack present in the network. The entire process is carried out in two phases. In the first phase, sink hole attack is implemented with slight modifications in the AODV protocol used. In the second phase, the attacked / malicious node is identified with the help of the trust based secure algorithm designed.

A.Phase - 1:

Initially a wireless sensor network is created with randomly distributed sensor nodes within the specified area. Then the main aim in phase 1 is to implement the sinkhole attack in to the network. Using AODV protocol the sinkhole attack is implemented by changing the sequence number in route request packet. Higher sequence number implies that the route through that particular node is shorter and the best to reach source. The attacker node carefully observes the sequence number of the source node from the route request packet of the source node. Then it generates a fake/duplicate route request packet with higher sequence number than the source node and starts broadcasting. The nodes that take this duplicate route request packet with higher sequence number feels that it is the shortest and fresh route to source than all others. Then eventually a path is created between source node and destination node through the sinkhole node. If once the path is set, then source starts sending the packets to destination through the sinkhole node, where it attracts all the data from the neighboring nodes and perform selective forwarding / packet dropping / data modification that results in abnormal behavior of the of the system.

Thus, in the first phase, a sinkhole attack is implemented successfully within the wireless sensor network.

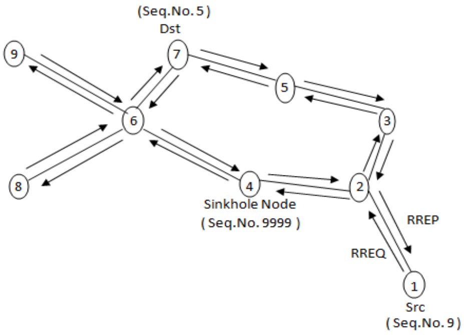

Fig.1 RREQ and RREP in sinkhole attack.

B.Phase - 2:

The main idea of second phase is to detect the sinkhole attack present in the network. For this process to begin, initially neighbor database construction takes place, where Base station sends the HELLO packet to its neighbor nodes that includes node_ID and hop count fields in it. To begin with base station, it has zero hop count. The node that receives the packet will update its node_ID and hop count from the base station and replies back. The faraway nodes that receive the packet through intermediate nodes will give its node_ID and hop count from the base station (given by the no. of nodes present in between the intended node and the base station). At the end of the process, base station possess complete database of the nodes present in the network. To identify the sinkhole attack in the wireless sensor network, each sensor node sort its database using any sorting algorithm. But sorting should be done based on the hop count from the base station. Then separate the lowest hop count value and corresponding ID. Even if there exists many more copies of the lowest hop count, separates them all. Then it calculates the average value of the rest of the hop counts. Then finds the difference (%) between lowest hop count and average value to make a decision on sinkhole node. If difference % is greater than the threshold, then it is detected as the sinkhole attack and if not, it is a normal working node. Once if the attack is found, it informs to other nodes and base station regarding the malicious node.

Difference (%) = [(Avg. Hop – Low. Hop) ÷ Avg. Hop] × (100 %). (3.1)

IV. Simulation and Results

The proposed algorithm was simulated using NS – 2 simulation software. This is because the software is very much flexible to operate on wireless sensor networks. Also, it helps in identifying the pros and cons of a designed network before being implemented in real time. Here, the output is shown in two different forms as follows :

The following output shows the formation of the general wireless sensor network and the packet transmission between the source and destination through some other intermediate nodes.

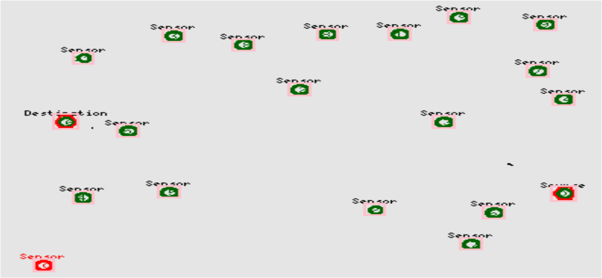

Fig.2 Network Before detecting the attack.

The following output shows the scenario after detecting the sinkhole node present in the network. This is obtained after implementing the final algorithm designed to detect the sinkhole attacks present in the network.

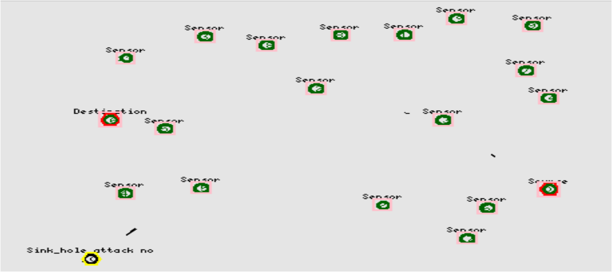

Fig.3 Sinkhole Attack Detection.

In the above figure, the node represented with yellow circle is the sinkhole node that which is attracting the data from the neighbor nodes and dropping / modifying it. Thus, it is found as the malicious node and detected as a sink hole attacked node.

V. Conclusion

There are many algorithms proposed before for detecting the sinkhole attacks in the wireless sensor networks. Also many of those were mainly aimed to detect the attack alone. But, in this paper, we proposed a better algorithm that which could detect the sinkhole with much possible accuracy. The other main thing to keep noticed in wireless sensor networks is the energy parameter. As we all know, the sensor nodes are possessed with limited energy source which makes a tough task to go through while designing an algorithm related to wireless sensor networks.

Here in this paper, we designed a secured and trust based new algorithm that detects the sinkhole attack based on the hop count. Also, implementing this algorithm doesn't let the node energy drain unnecessarily as it doesn't require any hardware unit to execute. The only complication present is sorting and calculating the average. But these can be easily done with the kind of advancement present in designing a sensor node. Furthermore, the work can be carried with some other parameter to detect attack and can look to reduce the complications present in the algorithm and can help providing a better energy efficient and trust based algorithm to detect the sinkhole attack in wireless sensor network.

VI. References

1. A Survey on Centralised and Distributed Clustering Routing Algorithms for WSNs (PDF). IEEE 81st Vehicular Technology Conference. Glasgow, Scotland: IEEE. Spring 2015. doi:10.1109/VTCSpring.2015.7145650. Retrieved March 4, 2016.
2. I. F. Akyildiz and I.H. Kasimoglu (2004). "Wireless Sensor and Actor Networks: Research Challenges". Ad Hoc Networks 2 (4): 351–367. doi:10.1016/j.adhoc.2004.04.003.
3. I.F. Akyildiz, W.Su, Y.Sankarasubramaniam, et al, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, 2002.
4. O.Younis, M. Krunz and S. Ramasubramanian, "Node clustering in wireless sensor networks: recent developments and deployment challenges", Network, IEEE, vol 20, Issue 3, pp. 20 – 25, May-June, 2006.
5. D. Sheela, Nirmala. S, SangitaNath and Dr. G Mahadevan, "A Recent Technique to Detect Sinkhole Attacks in WSN".
6. Ad hoc On-Demand Distance Vector (AODV) Routing ietf-draftmanet- aodv-13.txt.