JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Distributed Fault Aware Routing Protocol towards Eliminating Sink Hole and Worm Hole Attacks in wireless Sensor Network

M.Malathi.,M.Sc.,M.Phil., **Dr. A. Senthil kumar.,M.C.A., M.Phil.,**

Abstract

Wireless Sensor Network composed of sensor nodes has an ability to periodically communicate its sensed data containing their specific environment information with base station through mobile sink. As sensor node is resource constrained, energy balancing techniques have been growing significantly in recent years using cluster based technique. However security issues have limited focus in the existing literatures which makes network vulnerable to various types of attacks propagation in the network including wormhole and sinkhole attacks. These attacks block the effective communication of the nodes to sink with false information towards transmitting the sensed data to base station. In order to defense the network against wormhole and sinkhole attacks, a security solution has been proposed in this article. A Distributed Fault Aware Routing (FAR) protocol, a new security scheme developed to detect and resist both sink hole and wormhole attack at same time in the various layers of network. Fault Aware routing mechanism uses the voting method in the Adhoc on Demand Multipath distance routing protocol. The voting methods compute the fault occurring in terms of security violation. It uses the Minimum Mean Squared Error Estimation (MMSEE) on the each node and its neighbors to identify the node with false energy and location information in the network. In addition, sink hole attacked node projects the false hop count to the sink. On identification of MMSEE value of the nodes, fault aware routing protocol identifies the attacking nodes and it eliminates it from further propagation in the network to provide better energy utilization and less data loses. The simulation analysis of the proposed network protocol is carried out and tested in the network simulator 2. The simulation results proves that it proposed secure routing protocol is capable of eliminating the wormhole and sinkhole attacks with high energy consumption and less hardware size on comparing against traditional cryptographic based secure routing protocol.

Keywords: Wireless Sensor Network, Wormhole Attack, Sinkhole attack, Adhoc on Demand distance Vector Routing protocol, Fault Aware Routing

1. Introduction

Wireless Sensor Networks (WSNs) have gained significant interest among research communities due to its utilization on monitoring the specific environment and it is adapted for wide number of applications such as health monitoring system, real time traffic monitoring and habitat monitoring etc in more convenient ways. Further it lacks infrastructure in data communication of its sensed information to the base station[1]. The base station is used to collect the sensed information as it contains high computational and storage abilities than sensors. However WSN have limited battery power and limited capabilities which bring major challenges in energy preserving and to defense the network against various attack propagation[2]. Therefore, it is very critical to provide security especially to wormhole and sinkhole attack as deployment of the network in public locations where attacker can capture the sensed information due less secure data communication channels. Defending the wormhole attack[3] and sinkhole attack[7] is emerging trend in self organizing network which leads to a design of effective secure routing technique on incorporating all those constraints.

In this paper, a Fault Aware Routing (FAR) protocol has been developed to identify and mitigate the both sinkhole and wormhole attack. In order to achieve strong security, voting mechanism on Adhoc on Demand Multipath distance routing protocol has been employed to compute Minimum Mean Squared Error Estimation (MMSEE) value. The MMSEE value compute the node reputation on basis of node information provided to path estimation by normal node and fake node towards data routing to base station through mobile sink. The estimation of node reputation eliminates the false energy and false location information of the projecting node. Further it identifies the misbehaving node with characteristics of wormhole characteristic and sinkhole characteristics and eliminates those nodes from further data communications. This solution provides sensor nodes to have better data communication to sink node with high impact on network life time due to energy utilization.

The rest of this paper is organized as follows: Section 2 describes various security related routing techniques for Wormhole attacks in WSN. Section 3 provides the design of proposed secure routing protocol towards eliminating the wormhole and sinkhole attack in parallel. Section 4 provides simulation setup and performance analysis of the secure routing technique against traditional security scheme on basis of data loss, packet delivery ratio and energy utilization. Finally, Section 5 concludes the paper.

2. Related Work

In this section, various literatures related to secure routing technique against the various attacks in the wireless sensor network was discussed on multiple aspects is as follows

2.1. MAC based Centralized Routing Protocol (MCRP)

In this literatures, 802.15.4 wireless sensor network (WSN) has been utilized to calculate and deliver routing paths, monitor the network topology and perform other energy-intensive tasks. MCRP is a reactive routing protocol to detect wormhole attacks on the utilization of the information on the nodes' locations. It uses iterative Least Trimmed Squares (LTS) approach to identify the wormhole attacks with respect to beacon messages[4].

3. Proposed model

In this part, definition of the attack and its attack characteristics along network design to eliminate those attacks has been provided in detail.

3.1.Definition of the Attacks

In this section, definition of the various attacks propagating in the network is defined and its behavior characteristics are highlighted.

- **Wormhole Attack**

It is considered as attack which consists of two or more malicious nodes for data communication on establishing a tunnel. The maliciousnodes obtain the data packets from one location of the node and transmit to other distant located node through established tunnel with or without hops. The tunnel constructed in both form as In bound and Out bound channel to transfer the collected sensed information in multi-hop routes. The data communication through tunnel achieve faster data transmission rate with less no of hop compared to other normal data packet communication in the network[5].

- **Sinkhole Attack**

It is considered as attack which consists of one or more malicious node for blocking the data communication between the sensor nodes and the sink on falsely advertising it as sink. It carried out by providing false hop count to the sink which is smaller than its actual hop count to the sink. Further neighbor node transform the data to malicious node as it consider as shorter route to sink. The sinkhole node's energy is infinite[8]**.**

3.2.Network Model

Wireless sensor network model composed of sensor node are randomly deployed with radius R and density P. A sink node is deployed in the center, and its energy is infinite. The sensor node is assigned with unique ID in the fixed location L (x_i,y_i) for gathering the sensed information and transmits to the sink node on identifying the shortest path. The sensor network is of event-monitoring type. After an event occurs, the node that detects the event will generate a packet and forward it according to the prescribed routing scheme[6].

3.3. Node Clustering and Cluster Head Selection

Node clustering is carried out using LEACH protocol to arrange the sensor node in form of cluster. To select the cluster head on each cluster, K-means algorithm is employed to dynamically select a Cluster Head on basis of the residual energy of the node and the distance from the node to the centroid in a cluster. It is produces effective energy consumption model. Each node is employed to voting approach to determine the behaviour of the node in the network[9].

3.4. Fault Aware Routing

Fault aware routing protocol is designed as secure routing protocol to the wireless sensor network to withstand against the multiple malicious network attacks. It utilizes the computation of the Minimum Mean Squared Error Estimation in the voting based approach and Adhoc on Demand Multipath distance routing protocol to data communication to base station through sink

3.4.1. Minimum Mean Squared Error Estimation (MMSEE)

It is alterative and distributed method computes the Minimum Mean Squared Error Estimation on each node on obtaining the information of neighboring reference nodes. It utilizes the distances difference measurement among the location references from anchor nodes to identify and remove malicious ones with respect to defined threshold confidence value. The distance measurements between normal sensor nodes and its neighbor node are defined as dist (Si, Nj)

$$\text{dist (Si, Nj)} = \| s_i - n_j \| + \mu_{ij} \quad \text{Nj} € \text{p}$$

This measurement determines the outliers of the node so that it can produce trustworthy position estimates on basis of the confidence value and its error of all available sensor nodes. Figure 1 represents the architecture of the proposed model.

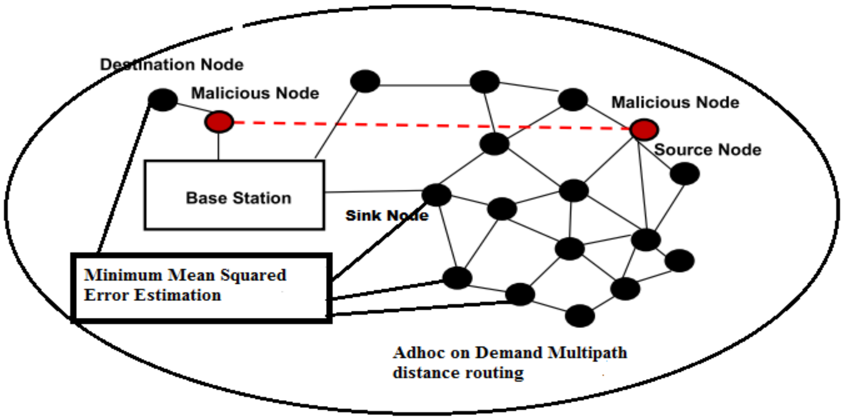
Destination Node
Malicious Node
Malicious Node
Source Node
Base Station
Sink Node
Minimum Mean Squared Error Estimation
Adhoc on Demand Multipath distance routing

Figure 3.1: Architecture Secure Routing Technique –Fault Aware Routing

- **Condition to Determine Wormhole Attack**

Node Density N_s of Sensor node and its Neighbor node & Compute Node Radius r of Sensor Node and its Neighbor Node

If (Node Density N_s of Sensor Node > Confidence Value MMSEE)

$$\text{Node Radius} = \tanh[\frac{q-B(t)\sin k(ct)}{\cos K(ct)}$$

$$\text{Node radius} > 2a_0 + MaxD(s)n\sum_{n=1}^{\infty}\left(a_n\cos\frac{n\pi x}{L} + b_n\sin\frac{n\pi x}{L}\right)$$

Node is considered as Wormhole

Algorithm 1: Wormhole Detection

```
Input : x, dist($S_i$ , $N_j$) dist($N_i$ , $N_j$)
Set $p_i$ =0,
Set $N_i$ =0
For( i=1 &&  I <n)
  Compute Malicious Neighbour node cluster
While ($ND_{jt<}ND_{it}$)
   Estimate senor nodes Nr dist($S_i$ , $n_j$) of Max(D)
Output: Malicious nodes NM
```

- **Condition for Sinkhole Attack**

Hop Count of $N(i)_s$ considerer $H(i)_s$

Hop count of N(i)s computed as

$$H(i)_s = (1+x)^n = 1 + \frac{nx}{1!} + \frac{n(n-1)x^2}{2!} + \cdots + \sum_{k=0}^{n}\binom{n}{k}x^k a^{n-k}\pi r^2$$

```
If (sink distance from Sensor > Threshold Value)
  Compute Hop Count of Neighbor to Sink
  IF (Hop Count of Neighbor< 1&& Distance of source node >Minimum Distance Threshold )
   Compute Node as Sinkhole Node
```

Algorithm 2: Wormhole Attack

```
Input (Node (i), $d_{min}$, $d_{max,}$ $H(i)_s$)
Output
Process
Senor broadcast RREQ to all nodes for routing path
          Nodes receive a message from all node RRQP
          Nodes send a status message to all nodes with less Hop Count
Calculate the distance length of the sensor node to sink node
          $H(i)_s = (1 + x)^n = 1 + \frac{nx}{1!} + \frac{n(n-1)x^2}{2!}$
If (No of hop to sink node to sensor node < Threshold)
        Node is sinkhole node
```

3.4.2. Adhoc on Demand Multipath distance routing protocol

Ad-hoc on-demand Multipath Distance Vector routing protocol (AOMDV) is used to discover multiple paths between the source and the destination for contending link failure with reference to routing table which contains energy and packet transmission information. It will select the main path for data transmission which is based on the time of routing establishment on computation of MMSEE along wormhole and sinkhole characteristics[10]. Further Malicious Node is eliminated on routing protocol with node IDwhich produces dropping and eavesdropping attack.

4. Simulation Results

Simulation Analysis of the proposed secure routing protocol is carried out using NS2 Simulator with simulation parameter as defined with table 1. The performance is computed with respect to 10 nodes, 25 nodes, 35 nodes and 45 nodes. The performance of the proposed model is computed on measures such as throughput, end to end delay and packet delivery ratio.

Parameters	**Values**
Simulation Area	500m*500m
Routing Protocol	AOMDV
Packet Size	512 bytes
Mobility Model	Fixed
Range of	230m

transmission	
Simulation Time	200s

The performance analysis of attack detection in the proposed work is carried out on various intervals. Figure 2 provides the performance analysis proves that proposed model achieves high throughput on comparing with existing technique on changing no of nodes in simulation. It proves effective for wormhole and sinkhole attack.

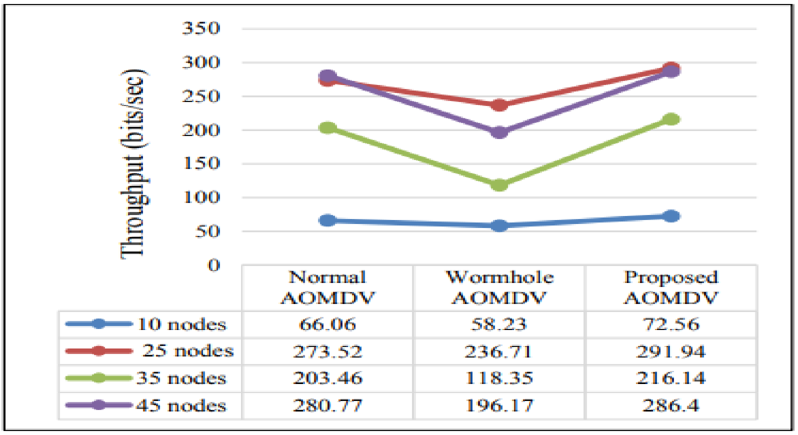

Figure 2: Performance analysis of the Secure Routing Protocols

Moreover, the packet loss rate in the proposed detection scheme is less than that in the existing detection schemes and it has been proved that it achieve good performance on various performance measures.

Conclusion

Distributed Fault Aware Routing (FAR) protocol for eliminating the wormhole and sinkhole attack has been designed and implemented. Proposed protocol determines the Minimum Mean Squared Error to set effective threshold to eliminate the attack propagation in the network. The model identifies the malicious node with respect to false hop count, energy information and location data effectively. Further it provides effective defense on seamless identification of attack characteristics. Finally, experimental results demonstrate that the performance of the proposed scheme is better than that of existing schemes especially for energy utilization, throughput and data loss.

References

[1] S. Bhagat and T. Panse, ‘‘A review on detection and prevention of wormhole attack in wireless sensor network,’’ Int. J. Comput. Appl., vol. 127, no. 13, pp. 1–4, Oct. 2015.

[2] G. Farjamnia, Y. Gasimov, and C. Kazimov, ‘‘Review of the techniques against the wormhole attacks on wireless sensor networks,’’ Wireless Pers. Commun., vol. 105, no. 4, pp. 1561–1584, Apr. 2019.

[3] A. P. Rai, V. Srivastava, and R. Bhatia, ‘‘Wormhole attack detection in mobile ad hoc networks,’’ Int. J. Eng. Innov. Technol., vol. 2, pp. 174–179, Aug. 2012.

[4] P. Amish and V. B. Vaghela, ‘‘Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol,’’ Procedia Comput. Sci., vol. 79, pp. 700–707, Jan. 2016.

[5] T. Minohara and K. Nishiyama, ‘‘Poster: Detection of wormhole attack on wireless sensor networks in duty-cycling operation,’’ in Proc. Int. Conf. Embedded Wireless Syst. Netw., Feb. 2016, pp. 281–282.

[6] Y. J. Zhu, Y. Q. Li, Q. G. Fan, and Z. Wang, ‘‘Ad hoc on-demand distance vector routing protocol based on load balance,’’ in Proc. MATEC Web Conf., 2016, Art. no. 02090.

[7] NK. Sreelaja, GAV. Pai, "Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks", Applied Soft Computing, vol. 19, pp. 68-79, 2014.

[8]L. Sánchez-Casado, G. Maciá-Fernández, "Identification of contamination zones for sinkhole detection in MANETs", Journal of Network and Computer Applications, vol. 54, pp. 62-77, 2015

[9] G. Jahandoust, F. Ghassemi, "An Adaptive Sinkhole Aware Algorithm in Wireless Sensor Networks", Ad Hoc Networks, vol. 59, pp. 24-34, 2017.

[10] M. Abdullah, MM. Rahman, MC. Roy, "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count", International Journal of Computer Network & Information Security, vol. 7, no. 3, pp. 50-56, 2015.