I J C T A, 9(2) 2016, pp. 557-564

Decentralized Detection and Mitigation of Sinkhole Attacks in Wireless Sensor Networks based on Network Density Estimation Technique

K. Devibala[1], S. Bala Murali[2] and S. Venkateselu[3]

ABSTRACT

The modern Wireless Sensor Networks (WSN) has wider perspective implication in various domains but the frequency of network threats also grown with the technology. Apart from other threats, the traffic orient sinkhole attack makes the remarkable difference in quality of service in any service orient architecture. By learning traffic, the sinkhole nodes reduce the scalability and performance of the whole network. Identifying the presence of sinkhole attacking nodes and mitigating them is the great deal of research in wireless sensor network; we motivated with the challenge and propose a novel decentralized sinkhole detection mechanism using Network Estimation Technique (NDE). The NDE technique is performed by every node of the network where every node maintains the neighbor table to store the neighbor details. Also the node monitors and computes the average traffic occurred in its own interface at each time window. The own traffic has been estimated based on number of packets being received at each time domain, whether it belongs to the same or others. With the computed traffic, the node collects the information about the neighbors of neighbor nodes. Using all these NDE techniques estimate the network density and identifies the presence of malicious node in the region. Identified malicious node information is distributed to the neighbor nodes, so that the malicious node will be ignored at next transmissions. This method reduces the overhead of collecting snapshots and routes. This method increases the network throughput by increasing the Best Effort (BE) traffic.

Keywords: BE Traffic; WSN; Sinkhole attack; Density Estimation.

I. INTRODUCTION

The WSN is a collection of number of mobile nodes formed as a network without any topology constraint. The nodes of the network will be keeping change at all the fraction and the snapshot of the network is varying continuously [10]. The packet sent from a source towards any destination will be forwarded by the intermediate nodes. The selection of forwarding node is preferred support on the routing protocol engaged in the network [6]. There are many routing approaches available to route packets between different nodes of the network.

The intermediate nodes perform forwarding of packets towards destinations and there are nodes which try to capture the packets flow in the network. Using captured packet, the node can infer or identify various network related information or some sensitive information [7]. That node is represented as a malicious node and the source node will request for routes to reach the destination to all its neighbors. The neighbors perform route discovery and reply with set of routes. What the malicious node will do is, it will return the source node as it is the shortest route available in the network. By seeing this, all the nodes will send the packets through the malicious node which cause energy depletion in some point of the node near sink node. This is named as sinkhole attack, which reduces the network life time and performance of the network.

[1] Department of Computer Science, Ayya Nadar Janaki Ammal College, Sivakasi, Tamilnadu, India

[2,3] Department of computer Application, Kalasalingam University, Krishnankoil, Tamilnadu, India, *E-mail: sreebalahoney@gmail.com*

The BE traffic is one which utilizes the bandwidth and distributing the traffic all over the network uniformly [3]. The routing protocol has to optimize the energy constraints of the nodes of network and has to select the route based on the traffic present in each possible route. The BE traffic increases the lifetime of the network. The density of the network can be computed using different measures; any sensor node has fixed transmission range within which it can transmit the packets to the nodes of network. If the neighbors of a node and their neighbors with the location details can be collected then using the geographic region and their locations we can estimate the density of the region. Once the density of any region has been estimated then with the help of transfer frequency or flow estimation any node can identify the impact of sinkhole attack.

II. RELATED WORK

There are many approaches those have been discussed in the literature for detection of sinkhole attacks in WSN. We review few of them in this section which are relevant to our problem. Detection of sinkhole attack in wireless sensor networks [8] proposes a Sybil attack detection scheme which initially uses the consistency of data to find the group of suspected nodes. Then, the trespasser is acknowledged capably in the group by checking the network flow in sequence. Accurateness and effectiveness of the algorithm have been estimated by using numerical analysis and simulations.

Intrusion recognition of sinkhole attacks [9], proposes a novel algorithm for detecting sinkhole attacks for large-scale WSNs. They formulated the detection problem as a change-point detection problem. Specifically, they monitor the CPU usage of each sensor node and analyze the consistency of the CPU usage. Thus, the algorithm is able to discriminate among the malicious and the genuine nodes. A sinkhole attack recognition scheme in Mintroute wireless Sensor Networks [10], offers the vulnerabilities of Mintroute protocol to sinkhole attacks and the existing manual rules used for detection are considered using different planning.

An Approach to build up the Performance of WSN during Wormhole Attack using Promiscuous Mode [1], proposes method to sense and detach the malicious node during wormhole attack. This paper proposed that the nodes which are not take part in multi-path routing, create an alarm message during interruption and detach the malicious node from network. Detection and defense of Sinkhole attack in Wireless Sensor Network [11], realizes a mechanism to launch sinkhole attack at WSNs and then present some mechanisms to detect and defense this type of attack. Finally, they did some experiments to verify their methods.

Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques [12], deals with a position and neighbor discovery protocols, mislead to an isolated remote WSN node into believing that it is a neighbor of a set of local nodes was carried out by providing two colluding nodes to set a wormhole. In this paper, detects the wormhole attacks using range-free methods (DWARF) under which they derived two specific wormhole detection schemes: the first approach, DWARF Loc, carry out mutually the detection and localization procedures make use of range-free techniques, while the other, DWARF Test, uses a range-free method to make sure the legality of the estimated situation of a node once the position discovery protocol is completed [2].

A non cryptographic method of sink hole attack detection in wireless sensor networks, proposed a scheme to defend against sinkhole attacks using mobile agents. Mobile agent is a program segment which is self controlling. They navigate from node to node not only for transmitting the data but also doing computation. They are an effective pattern for distributed applications, and especially attractive in a dynamic network location.

A routing algorithm with various restraints is projected based on mobile agents [4, 5]. It uses mobile agents to gather information of all mobile sensor nodes to make every node conscious of the whole network so that a valid node will not listen the cheating information from malicious or compromised node which guides to sink hole attack. The important feature of the proposed mechanism is that it does not need any encryption or decryption mechanism to detect the sinkhole attack. All the above approaches have the problem of identifying the malicious nodes effectively.

III. PROPOSED METHED

The proposed method has various stages of sinkhole detection and the mitigation is performed in different steps. The functional components of the proposed model can be named as Neighbor Discovery, Neighbor Density Estimation, and Sinkhole Detection. The ND is carried out to gather the information regarding the two hop neighbors, NDE is to act upon density estimation, and used to identify the presence of malicious nodes in the networks.

(A) Neighbor Discovery

Every node in the network performs neighbor discovery whenever there is a packet to be transmitted. The node put up a hello message and transmits into the network and the node which obtains the message situated within the communication range of the source node will reply with Hello Reply. The Hello reply consists of various information like, the number of neighbors, node ID of neighbor, location details, number of messages transmitted, number of messages received, energy depletion occurred and so on. All these information are kept in the hello reply and sent to the source node. This source node receives all the reply which arrives within certain time and extracts the details to perform density estimation.

Algorithm

```
Input: NULL
Output: Neighbor Details ND.
Step1: Start
Step2: Construct Hello Message HMSG.
Step3: Broadcast the Hello Message HMSG.
Step4: Initialize Broadcast Timer
    While (Timer==True)
        Receive hello reply HREP.
    Extract the neighbor features from HMSG.
        Number of neighbors NN = $\int \Sigma Node \in HM$
        Node ID of neighbors NID = $\int \Sigma Node.ID \in HM$
        Location of Nodes LoC = $\int_{i=1}^{NN} Location(NID) \in HM$
        Number of packet Received NR = $\int_{i=1}^{NN} NR(NID) \in HM$
        Number of packet Transferred NT = $\int_{i=1}^{NN} NT\,(NID) \in HM$
        Energy of node ED = $\int_{i=1}^{NN} ED(NID) \in HM$
    End
Step 5: Generate Node History
    For all node id $NID_i$ from NID
            ND(i) = {NN,NID,LoC,NR,NT, ED}.
    End.
Step 6: stop.
```

(B) Neighbor Density Estimation

The neighbor density is estimated using the neighbor history or neighbor details obtained from different neighbor of the node. From the collected information, the overall geographic region is computed and based on the area computed with the number of nodes in the region, we estimate the network density. The estimated density value is used to suspect the presence of sinkhole node in the network. If the density is less than a threshold which is computed based on geographic and number of nodes then it is concluded that there exists a malicious node.

Algorithm

```
Input: Neighbor History ND.
Output: Sinkhole Flag.
Step1: Initialize sinkhole flag to false.
Step2: Compute area of overall transmission AT.
AT = $\int_{i=1}^{NN} \forall (Loc) \times \sqrt{X\ Loc1.X^{2} + Loc2.Y^{2}}$
Step3: Compute Density of region.
Dn = $\frac{AT}{NN} \times 100$
Step4: Compute number of nodes has minimum traffic
NMT = $\int \Sigma\, Node\left(\frac{NT}{NR}\right) > Min\,Traffic$
Step5: If Dn>DensityThreshold && NMT>0
          Return flag.
Step6: Stop.
```

(C) Sink-Hole Detection

The sinkhole is detected in a distributed manner, where each node computes its own estimation of Neighbor Density. The sinkhole is identified based on the traffic pattern of all neighbors. In this approach for each neighbor and their neighbors we compute the average Traffic Introduction Factor (TIF) which is computed based on the number of packets being sent or received by all the nodes considered. The TIF represents that how well a node has been participated in the transmission and so on. Based on the TIF, we can conclude that the node is malicious or not. The node which has more TIF, with the neighbors which has less TIF than the Transmission Range (TR) threshold is used to identify the malicious node.

Algorithm

```
Input: Neighbor History ND.
Output: Malicious Node MN.
Step1: Start
Step2: For each neighbor
    Compute traffic introduction factor TIF.
```

```
        TIF = $\int_{i=1}^{N} NID\left(\frac{(NR+N}{100}\times TR\right)$
        End.
Step3: For each neighbor
        Identify number of nodes with less TIF.
        NTIF = $\int \Sigma\, NID < TIF\ threshold$
  End.
Step4: Choose most weighted node
            N = $\int Max(TIF).N$
Step5: Compute available Routes to sink
        Rset = $\int Routes - To - Destination$
Step6: If N is shortest then
            Else
            N is malicious.
        End.
Step7: Stop
```

IV. RESULTS AND DISCUSSION

The proposed NDE based sinkhole detection and mitigation technique has been implemented in NS2 and tested for its effectiveness in all the measures of quality of service. The method has been simulated with different scenarios with different number of nodes. The simulations were approved out using a WSN setting consisting of 100 wireless nodes over a simulation area of 1000 meters x 1000 meters flat space working for 60 seconds of simulation time. In the simulation each node has been considered with same set of transmission range of 100 meters and the malicious nodes are assigned with the transmission range of 500 meters.

Table I
Parameters Used in Our Simulation

Constraint	*Value*
Version	Network Simulator-allinone 2.34
Protocol	NDE (Network Density Estimation)
Area	1000m x 1000m
Transmission Range	100 m
Traffic model	User Datagram Protocol, Constant Bit Rate
Packet size	512 bytes

Table 1, shows the simulation details used in this paper. The method has been simulated for its effectiveness in sinkhole detection with different topology and simulation parameters.

Table II
Comparison Results

S. No	*No. of Nodes*	*Protocol*	*Detection Rate*			
			False +ve	*False-ve*	*Throughput*	*PDF*
1.	100	Range Free	3.5	2.5	88	6.9
2.	100	Sera	3.0	2.0	88.2	5.5
3	100	Polygon	2.8	1.8	90.5	4.9
4	100	G-Hazard	1.3	1.0	92	3.6
5	100	NDE	0.4	0.3	99.6	1.2

Table 2, shows the comparison of results produced by different methods in most important factors of quality of service.

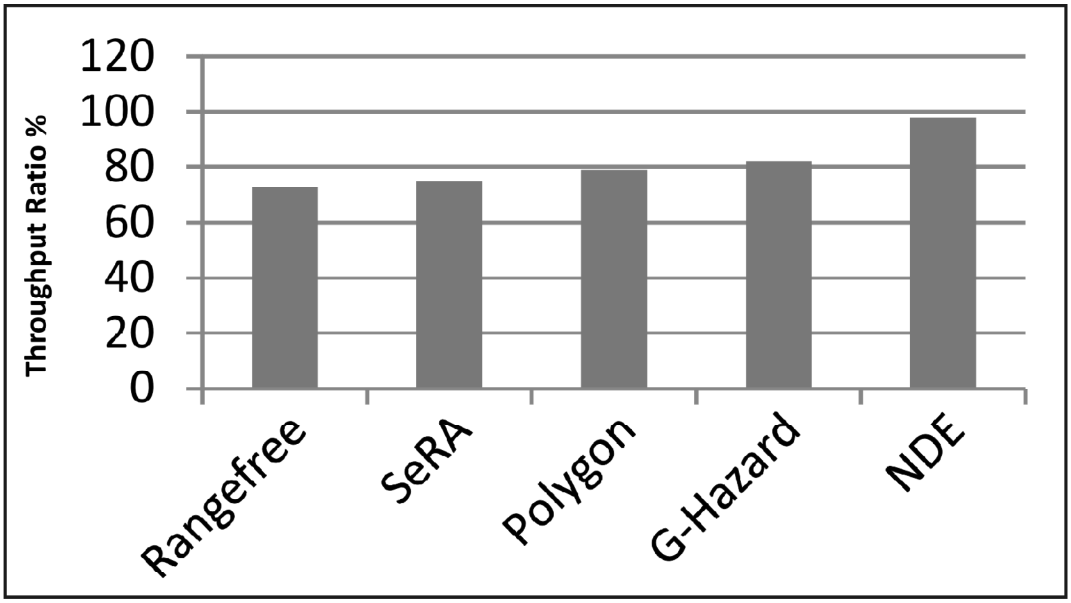

Figure 2: **Sinkhole Detection Accuracy**

Fig. 2. Shows the comparison of sinkhole detection accuracy. This result shows that the proposed method has produced efficient detection accuracy than the other approaches.

(A) Throughput Performance

Throughput is the rate of packets received at the destination successfully. It is usually measured in data packets per second or bits per second (bps).

Average throughput can be calculated by dividing the total number of packets received by the total end to end delay.

Fig. 3 shows the overall throughput ratio of different methods and it is clear that the proposed NDE method has achieved higher throughput than other methods.

(B) Packet Delivery Fraction

The packet delivery ratio defines the rate of data packets received at a destination according to the number of packets generated by the source node. The packet delivery fraction(PDF) is computed as follows.

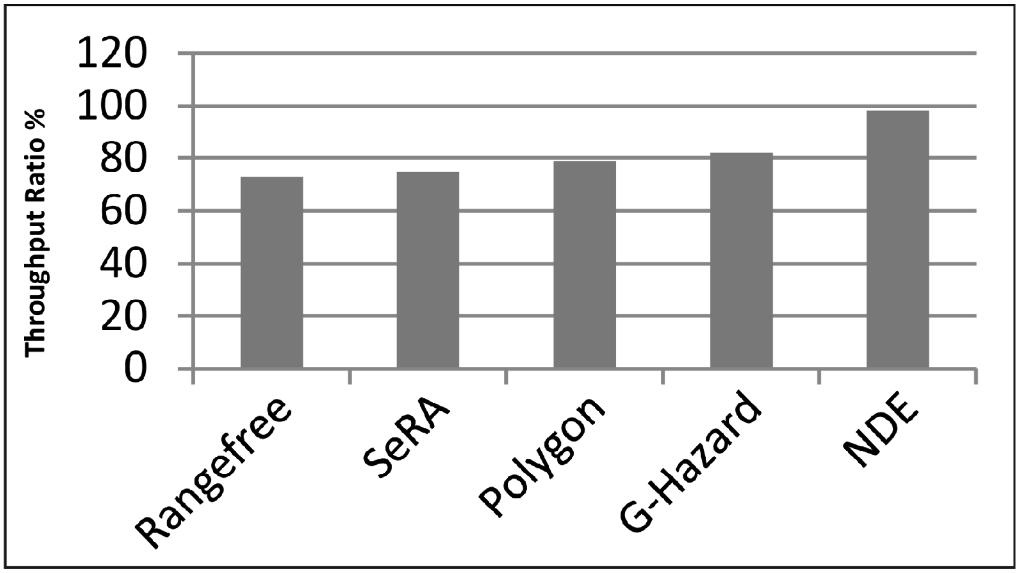

Figure 3: **Throughput Ratio**

PDF =(No. of packets Received/No. of Packets Sent)*100.

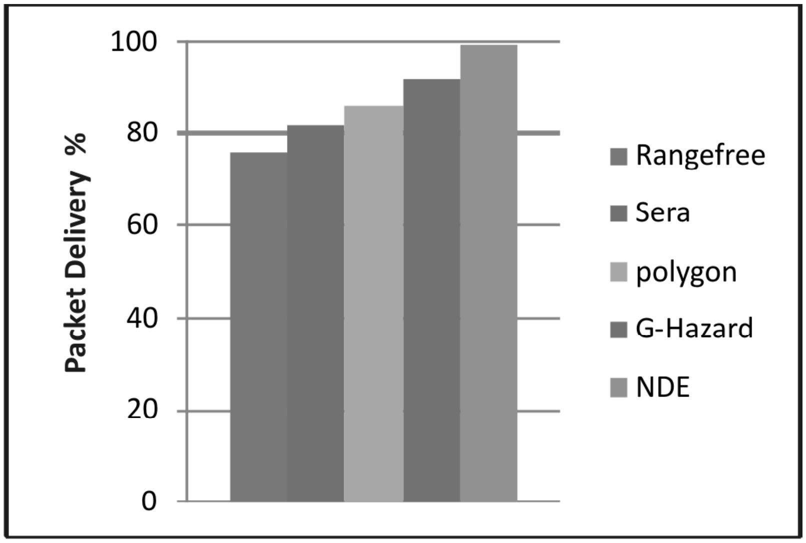

Figure 4: Packet Delivery Fraction

Fig. 4 shows the performance of packet delivery ratio of different algorithms and it shows that the proposed NDE method has higher packet delivery ratio than other methods.

V. CONCLUSIONS

In this paper, we have proposed a decentralized neighbor density estimation based sinkhole detection approach which reduces the overhead raised in earlier approaches. The node maintains the neighbor history and their information about their locations, number of packets being sent or received. Based on the details of neighbors, the neighbor density is estimated to suspect a node being malicious. The detection process is performed based on the traffic introduction factor which is computed based on packets being sent and received. Using the TIF a single node routes to reach the sink node or base station is computed. From the available routes the routes are verified to conclude the node is being malicious or not. The proposed method has reduced the overhead generated by distributed sinkhole detection process and produced efficient results.

REFERENCES

[1] Choi, M., Choo, H., “Bypassing hole scheme using observer packets for geographic routing in WSNs”, In: Proceedings of International Conference on Information Networking (ICOIN), IEEE, pp.435–440 2011.

[2] Shin, I., Pham, N., Choo, N., “Virtual convex polygon based hole boundary detection and time delay based hole detour scheme in WSNs”, In: Human Interface and the Management of Information. Designing Information Environments, vol. 5617, pp.619–627, Springer, USA, 2009.

[3] Baquero, C., Almeida, P., Menezes, R., Jesus, P., “Extrema propagation: Fast distributed estimation of sums and network sizes”, In: IEEE Transactions on Parallel and Distributed Systems vol. 23, pp. 668–675, 2012.

[4] Villalpando, R., Vargas, C., Munoz, D., “Network coding for detection and defense of sinkholes in wireless reconfigurable networks”, In: Proceedings of International Conference on Systems and Networks Communications (ICSNC’08), pp.286–291, 2008.

[5] Choi, B., Cho, E., Kim, J.; Hong, C., “Sinkhole attack detection mechanism for LQI based mesh routing in WSN”, In: Proceedings of International Conference on Information Networking (ICOIN), pp.1–5 2009.

[6] Krontiris, I., Dimitriou, T., Giannetsos, T., Mpasoukos, M., “Intrusion detection of sinkhole attacks in wireless sensor networks”, In: Algorithmic Aspects of Wireless Sensor Networks, vol. 4837, pp.150–161, 2008.

[7] Salehi, S.A., Razzaque ,M.A., Naraei, P., ”Farrokhtala, A.: Detection of sinkhole attack in wireless sensor networks”, In: Space Science and Communication (IconSpace), pp: 361-365, 2013.

[8] Changlong Chen., Min Song ., Hsieh, G., “Intrusion detection of sinkhole attacks in large-scale wireless sensor networks”, In: Wireless Communications, Networking and Information Security (WCNIS), pp. 711-716, 2010.

[9] Rassam, M.A., Zainal, A., Maarof, M.A., Al-Shaboti, M., “A sinkhole attack detection scheme in Mintroute wireless Sensor Networks”, In: Telecommunication Technologies (ISTT), pp. 71-75, 2012.

[10] Jin Qi ., Tang Hong ., Kuang Xiaohui ., Liu Qiang., “Detection and defence of Sinkhole attack in Wireless Sensor Network”, In: Communication Technology ICCT, pp:809-813, 2012.

[11] Mariano García-Otero., Adrián Población-Hernández., “Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques”, International Journal of Distributed Sensor Networks, vol. 20, 2012.

[12] Sheela, D., Naveen, K.C., Mahadevan, G., “A non cryptographic method of sinkhole attack detection in wireless sensor networks”, Recent Trends in information Technology (ICRTIT), IEEE, pp. 527-532, 2011.