VOL. 12, NO. 4, FEBRUARY 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

IMPROVING QUALITY OF SERVICE IN WIRELESS SENSOR NETWORKS USING NEIGHBOR CONSTRAINT TRANSMISSION CENTRIC DISTRIBUTED SINK HOLE DETECTION AND NETWORK SIMULATOR 2

K. Karthigadevi[1], S. Balamurali[1] and M. Venkatesulu[2]
[1]Department of Computer Applications, Kalasalingam University, Krishnankoil, Virudhunagar. India
[2]Department of Information Technology, Kalasalingam University, Krishnankoil, Virudhunagar, India
E-Mail: k.karthikrish@gmail.com

ABSTRACT

With the advances in technology, there has been an increasing interest in the use of wireless sensor networks (WSNs). WSNs are vulnerable to a wide class of attacks among which sinkhole attack puts severe threats to the security of such networks. The problems of sinkhole detection and mitigation have been studied through various methods, but suffer with the problems of high complex detection and overhead introduced by detection process. The quality of service has been degraded greatly by the impact of sinkhole attack because the malicious node can read much information about the source or the communications; this helps malicious nodes to perform various kinds of attacks. In order to overcome such drawbacks of network security, we propose a novel approach for sinkhole detection to support Quality of Service (QOS) development of wireless sensor networks. The method acts as a distributed one where the sinkhole detection is performed in all the nodes of the network. The node collects the neighbor information about the location and other transmission details. From the collected neighbor information, the node which presents in many nodes neighbor matrix is identified. The problem of multiple identification is resolved by verifying the transmission performed through other neighbors of the malicious node. From the traffic incurred in the neighbor of malicious node is used to verify the location or traffic sent by the malicious node. The method produces efficient results in sinkhole detection and increases the throughput. Also the method reduces the packet drop ratio and reduces the frequency of sinkhole detection.

Keywords: wireless sensor networks, sinkhole attacks, neighbor based detection, transmission centric approach, QoS development.

1. INTRODUCTION

The wireless sensor network (WSN) has the capability to be deployed in any point of time without any preparation. The WSN has a number of nodes which has mobility nature and could be used to form a network at many situations like war fields. The WSN are more useful in deploying the network in war filed and collect the information which will be used to perform various activities. Similarly the WSNs are useful in various situations to collect information. The nodes of the network perform both reception and transmission of packets for communication [1]. The co-operative communication is performed with the support of all the nodes of the network and there are some nodes which try to capture the packets being forwarded and learnt something from the packets. The learned information can be used to perform various network threats and the malicious nodes are capable of sending the packet direct to the base station [14]. This creates a set of energy holes around the base station which spoils the network life time and increases direct traffic to the base station. The sensor nodes maintain much information about the neighbors like their location, node id, and number of packets being sent and received. This information can be used to identify the false nodes. Every sensor node has a limited power and transmission range. The packet sent by any node can be received only by the nodes which are placed within the transmission range of the source nodes. If there is any node presents in the neighbor list of many nodes where they are apart geographically then we can say that the particular node is a malicious node [2].

The transmission centric approach can also be used to perform sinkhole attack detection and to identify the malicious nodes in the network [3]. The node or malicious node transfers the packet directly to the base station or to the node which is the most near to the base station [15]. What happens is if the malicious node transmits more packets then the intermediate nodes will not receive anything in that particular transmission. This information can also be used for sinkhole detection to support quality of service in WSN [20]. The quality of service is the key factor in WSN and the sinkhole attack reduces the throughput, and increases the packet drop ratio and latency.

2. RELATED WORK

There are many approaches those have been discussed in literature and we present some of them here which are relevant to the problem statement. Detection of wormhole attacks in Wireless Sensor Networks using range-free localization [4], suggests two wormhole detection procedures for WSNs, based on concepts working in a kind of range-free localization methods: one of the approaches performs the detection at the same time with the localization procedure, and the other operates after the conclusion of the location discovery protocol. Both approaches are effective in detecting wormhole attacks, but their presentation is fairly sensitive to shadowing effects present in the radio channels. Detection

and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool [6], uses a sequence number based sinkhole detection approach. The dispatcher node first requests the sequence number with the route request (RREQ), if the node receives this RREQ then replies its sequence number with route reply (RREP) message. Broadcasting node checks whether this will match with sequence number in its routing table. If it matches then information will be shared otherwise it will allocate the sequence number to the node. If the node recognizes the sequence number then the node will go through the network otherwise it will be eliminates from the network. Detection of sinkhole attack in wireless sensor networks [9] proposes a Sybil attack detection scheme which initially uses the consistency of data to find the group of suspected nodes. Then, the intruder is documented efficiently in the group by checking the network flow information. [21] The proposed algorithm demonstrates and evaluated by using numerical analysis and simulations. Therefore, accuracy and ability of algorithm would be verified. Intrusion detection of sinkhole attacks in large-scale wireless sensor networks [10], proposes an 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 proposed algorithm is able to distinguish between the false and the genuine nodes.

A sinkhole attack detection scheme in Mintroute wireless Sensor Networks [11], where the vulnerabilities of Mintroute protocol to sinkhole attacks are discussed and the offered manual rules which can be used for detection are examined using different architecture. [12] Estimates the area in the network where a sinkhole attack has occurred there by considering the energy consumption model in the network. [13] Then follows an entropy-based trust model in which more factors that affect trust computation are introduced. An intrusion detection system [16], called INTI (Intrusion detection of SiNkhole attacks on 6LoWPAN for InterneT of ThIngs), to identify sinkhole attacks on the routing services in IoT. Moreover, INTI aims to mitigate adverse effects found in IDS that disturb its performance, like false positive and negative, as well as the high resource cost. The system combines watchdog, reputation and trust strategies for detection of attackers by analyzing the behavior of devices and also another Intrusion Detection System (IDS) mechanism to detect the intruder in the network which uses Low Energy Adaptive Clustering Hierarchy [17] (LEACH) protocol for its routing operation. In the proposed algorithm, the detection metrics, such as number of packets transmitted and received, are used to compute the intrusion ratio (IR) by the IDS agent. Suggested work proposes two approaches to detect and mitigate such attack in WSNs.[18] It provides a centralized approach to detect suspicious regions in the network using geo statistical hazard model. Furthermore, a distributed monitoring approach has been proposed to explore every neighborhood in the network to detect malicious behaviors. In this work, propose a region based sinkhole detection approach which works using the neighbor conditions for the development of quality of service in WSNs [19].

3. METHODOLOGY

The proposed neighbor constrained traffic centric method has the following stages namely: Neighbor Centric Data Collection, Traffic Inference, and Sinkhole Attack Detection. The neighbor centric data collection is performed to collect the neighbor details and the traffic inference is performed to compute the participation of other nodes in the network. The sinkhole detection approach detections the presence of sinkhole and malicious nodes of the network.

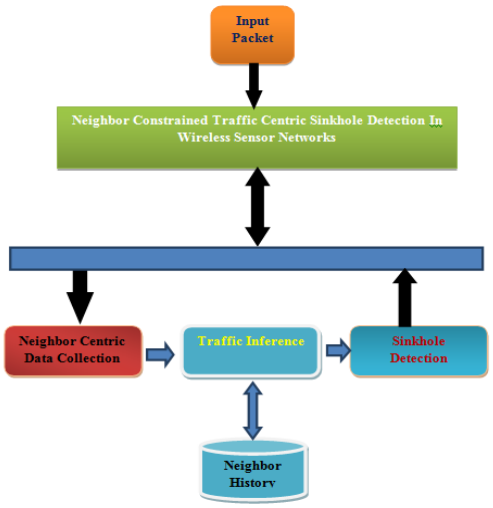

Figure-1. Block diagram of proposed architecture.

3.1 Neighbor centric data collection

The node of the WSN performs the data collection whenever it has a packet to be transmitted. The node constructs a Data Collection Message (DCM), and broadcasts into the network. The nodes are located in the broadcast range, and then source will accept the packet and reply with the Data Collection Message (DCMR) respond message. The reply has various information's about their location, transmission range, number of neighbors and their information, number of transmission performed and received. The features from the message will be extracted and stored to perform sinkhole detection later.

Algorithm:
Input: NULL
Output: Neighbor Information NI
Step1: Start
Step2: Construct DCM
Step3: Broadcast DCM
Setp4: While (True)
Receive DCM-Reply Message.
Extract the features from DCM-Reply.

Number of neighbors TN = $\int \sum Node \in DCMR$

Node ID of neighbors NodeID = $\int \sum Node.NodeID \in DCMR$

Location of Nodes NLoC = $\int_{i=1}^{TN} Location(NodeID) \in DCMR$

Number of packet Received TNR = $\int_{i=1}^{TN} TNR(NodeID) \in DCMR$

Number of packet Transferred TNT = $\int_{i=1}^{TN} TNT(NodeID) \in DCMR$

Energy of node ED = $\int_{i=1}^{TN} ED(NodeID) \in DCMR$

End

Step5: Generate Node History

For all node id NID_i from NID

ND (i) = {TNN, NodeID, NLoC, TNR, TNT, ED}.

End.

Step6: Stop.

3.2 Traffic inference

From the collected information about the neighbor nodes, we compute the traffic inference which represents the possibility of the neighbors participated in the transmission. There may be a malicious node located and could communicate directly to the sink node or base station. In order to monitor such a flow we compute the traffic inference which could be computed from the transmission performed by other nodes of the network. The inference is computed using the number of transmission performed by a single node which is suspected by the sinkhole detection process.

Algorithm

Input: Neighbor information NI

Output: Inference Flag IF.

Step1: Start

Step2: For each neighbor of Node N_i

Compute Traffic Rate Inference TRI.

TRI = $\int ND(\frac{(TNR+TNT)}{100})$

End.

Step3: Compute traffic rate of suspect node TRS= $\int ND(\frac{(TNR+TNT)}{100})$

Step4: if TRI<TRS then

Return true.

Else

Return false.

End.

Step5: Stop.

3.3 Sinkhole detection

The sinkhole detection is performed using the data collection and traffic inference model. The sinkhole detection is performed by each node of the network and the node identifies the malicious node as follows: Each node verifies the presence of multiple appearance of id in different nodes neighbor table and if there exist any id located in different nodes neighbor information then the traffic inference will be computed to conclude the sinkhole attack node. If there are many appearance of the same id in different nodes neighbor details the same is verified with the location details and inference model.

Algorithm

Input: Neighbor information NI

Output: NULL

Step1: Start

Step2: for each neighbor N_i from NI

Check for the appearance in multiple tables.

Count C= $\int_{i=1}^{size(NI)} Count(Ni, NI)$

If C>$\frac{2}{3} \times size(NI)$ then

Perform traffic inference TI

Flag F = TI (Ni, NI).

If F==True then

Declare Ni as malicious

Else

End.

End.

Step3: Stop

4. EXPERIMENTAL RESULTS

The proposed Neighbor Constraint Transmission Centric Distributed (NCTC) based sinkhole detection and mitigation technique has been implemented in Network Simulator 2(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 agreed out using a WSN atmosphere consisting of 100 wireless nodes over a simulation area of 1000 meters x 1000 meters flat space functioning 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-1. The constraint used in simulation.

Constraint	Value
Version	Network Simulator-allinone 2.34
Protocol	NCTC(Neighbor Constraint Transmission Centric)
Area	1000m x 1000m
Transmission Range	100 m
Traffic model	UDP(User Datagram Protocol), CBR (Constant Bit Rate)
Packet size	512 bytes

Table-1 illustrates the simulation details. The method has been simulated for its effectiveness in sinkhole detection with different topology and simulation parameters. Table-2 shows the comparison of results produced by different methods in most important factors of quality of service.

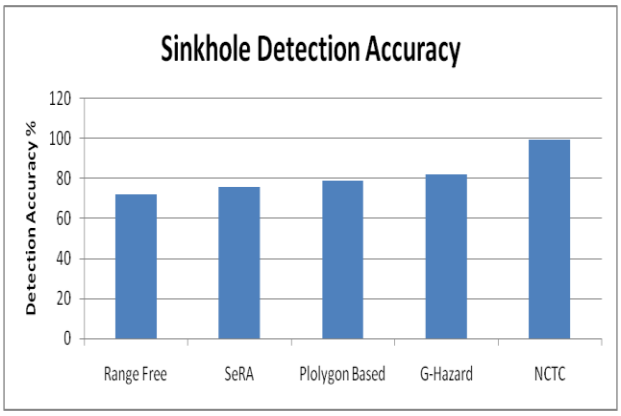

Figure-2. Comparison of sinkhole detection accuracy.

Figure-2 shows the comparison of sinkhole detection accuracy. The result reveals that the proposed method has produced more efficient detection accuracy than the other approaches.

4.1 Throughput performance

Throughput is the rate of packets arrived at the target successfully. It is regularly measured in data packets per second (dps) or bits per second (bps). Average throughput can be evaluated by dividing the total number of packets arrived by the total end to end delay.

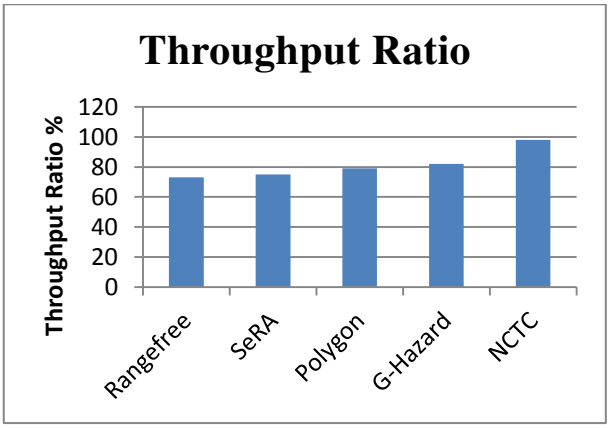

Figure-3. Throughput ratio of different methods.

Figure-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.

4.2 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. PDF (Packet Delivery Fraction) = (Number of packets arrived / Number of Packets dispatch)*100.

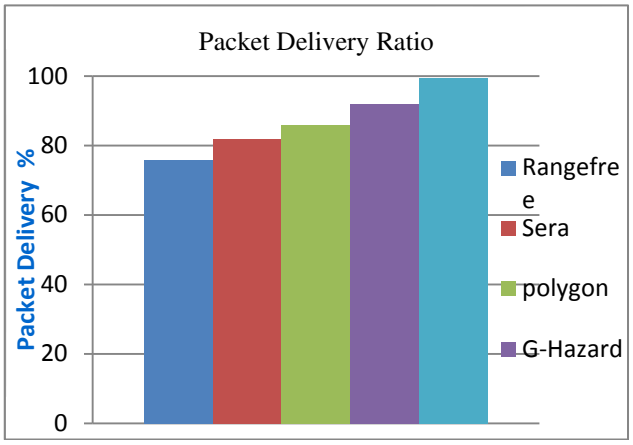

Figure-4. Packet delivery ratio.

Figure-4 shows the performance of packet delivery ratio of different algorithms and it indicates that the proposed NCTC method has higher packet delivery ratio than the other methods.

5. CONCLUSIONS

In this paper we have proposed a Neighbor Constrained Traffic Centric (NCTC) approach for sinkhole detection approach to get better quality of service in WSN. The node collects the information about the neighbors and their location, number of transmissions, receptions engaged. Similarly we compute the traffic rate inference based on the two measures the node is decided as genuine or malicious. The detection process is executed based on the traffic introduction factor which is calculated based on packets being sent and received. Using the NCTC 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] Yu F., Park S., Tian Y., Jin M. and Kim S. H. 2008. Efficient hole detour scheme for geographic routing in wireless sensor networks. In Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE. pp. 153-157.

[2] Choi M. and Choo H. 2011. Bypassing hole scheme using observer packets for geographic routing in WSNs. In The International Conference on Information networking. pp. 435-440.

[3] Shin I., Pham N. D. and Choo H. 2009. Virtual convex polygon based hole boundary detection and time delay based hole detour scheme in WSNs. In Symposium on Human Interface. pp. 619-627.

[4] García-Otero M. and Población-Hernández A. 2012. Detection of wormhole attacks in wireless sensor networks using range-free localization. In IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). pp. 21-25.

[5] Teng L. and Zhang Y. 2010. SeRA: a secure routing algorithm against sinkhole attacks for mobile wireless sensor networks. In Computer Modeling and Simulation, 2010. ICCMS'10. Second International Conference. 4, pp. 79-82.

[6] Singh T. and Arora,H. K. 2013. Detection and correction of sinkhole attack with novel method in WSN using NS2 tool. IJACSA. 4(2).

[7] Shukla P. K., Silakari S. and Bhadoriya S. S. 2009. Network Security Scheme for Wireless Sensor Networks using Efficient CSMA MAC Layer Protocol. In Information Technology: New Generations, Sixth International Conference. pp. 1579-1580.

[8] Singh H. and Malik G. 2011. Approaches to wireless sensor network: security protocols. World of Computer Science and Information Technology Journal (WCSIT). 1(7): 302-306.

[9] Krontiris I., Giannetsos T. and Dimitriou T. 2008. Launching a sinkhole attack in wireless sensor networks; the intruder side. In 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. pp. 526-531.

[10] Chen C., Song M. and Hsieh G. 2010. Intrusion detection of sinkhole attacks in large-scale wireless sensor networks. In Wireless Communications, Networking and Information Security (WCNIS). International Conference. pp. 711-716.

[11] Rassam M. A., Zainal A., Maarof M. A. and Al-Shaboti M. 2012. A sinkhole attack detection scheme in mintroute wireless sensor networks. In Telecommunication Technologies (ISTT), International Symposium. pp. 71-7.

[12] Hong Qi.J, Xiaohui T, K. and Qiang L. 2012. Detection and defence of Sinkhole attack in Wireless Sensor Network. In Communication Technology (ICCT), 2012 IEEE 14th International Conference on. 809-813.

[13] García-Otero M. and Población-Hernández A. 2012. Secure neighbor discovery in wireless sensor networks using range-free localization techniques. International Journal of Distributed Sensor Networks.

[14] Sheela D., Kumar C. N. and Mahadevan G. 2011. A non cryptographic method of sink hole attack detection in wireless sensor networks. In Recent Trends in Information Technology (ICRTIT), 2011 International Conference. pp. 527-532.

[15] Salehi S. A., Razzaque M. A., Naraei P. and Farrokhtala A. 2013. Detection of sinkhole attack in wireless sensor networks. In Space Science and Communication (Icon Space), 2013 IEEE International Conference. pp. 361-365.

[16] Naderi O., Shahedi M. and Mazinani S. M. 2015. A Trust Based Routing Protocol for Mitigation of Sinkhole Attacks in Wireless Sensor Networks. International Journal of Information and Education Technology. 5(7): 520.

[17] Cervantes C., Poplade D., Nogueira M. and Santos A. 2015, May. Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM) (pp. 606-611). IEEE.

[18] Sundararajan R. K. and Arumugam U. 2015. Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks. Journal of Sensors.

[19] Shafiei H., Khonsari A., Derakhshi H. and Mousavi P. 2014. Detection and mitigation of sinkhole attacks in wireless sensor networks. Journal of Computer and System Sciences. 80(3): 644-653.

[20] Fang-Jiao Zhang, Li-Dong Zhai, Jin-Cu Yang, Xiang Cui. 2014. Sinkhole attack detection based on redundancy mechanism in wireless sensor networks. Elsevier Procedia Computer Science. 31: 711-720.

[21] Tejindereep Singh and Harpreet Kaur Arora.2013. Detection and Correction of Sinkhole Attack with Novel Method in WSN using NS2 Tool. International Journal of Advanced Computer Science and Applications.