Asian Journal of Information Technology 15 (1): 156-161, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

Neighbor Condition Based Light Weight Region Based Approach for Detection and Mitigation of Sinkhole Attacks in Mobile Adhoc Networks

[1]R. Murugesan, [2]M. Vijayaraj and [3]K. Vetrivel
[1]Department of ECE, Ultra College of Engineering and Technology For Women,
625104 Madurai, India
[2]Department of ECE, Government College of Engineering 627007 Trinelveli, India
[3]Anna University Regional Campus, 641046 Coimbatore, India

Abstract: World looks more from wireless sensor network and the technology growth support for many things on the fly. We bothered at sinkhole attack generated on MANET and the quality of service which gets affected and disturbed. The success of network services only based on the quality of service metrics like throughput packet delivery ration, latency and many more. The problem of region based sinkhole detection is unhandled in the literature. We propose a sinkhole detection and mitigation mechanism to reduce the overhead generated by employing sinkhole detection at all the regions of the network. At first, the presence of sinkhole attack is identified using a novel method and then the region affected by sinkhole attack is identified and identified region is recovered using a light weight sinkhole detection mechanism. The proposed method works in centralized nature and overcomes the problem of deploying sinkhole detection process in distributed manner. The base station of the network maintains location information of all the nodes using which it computes the region and identifies the subset of nodes present in the affected region. The proposed method has been aimed at efficient energy utilization and increased throughput which have been achieved at higher ratio.

Key words: MANET, sinkhole attacks, location verification, QoS, network security

INTRODUCTION

Mobile adhoc network which runs on top of wireless communication where the nodes are assumed to perform sense and relay to support communication. The communication in MANET is performed in co-operative manner where each intermediate node supports data transfer by forwarding the packets to reach destination. As of wireless medium it's more less coupled network and prone to different kind of attack. There are different kind of attacks could be generated by malicious nodes, among them sinkhole attacks are the most important one which affects the quality of service of the network.

The communication in mobile adhoc network is performed in cooperative manner and the neighboring nodes supports data transfer by forwarding the packets to reach destination or base station. What the adversary will do is, whenever a node has some data to be transferred, it computes the least overhead path to reach the base station by performing neighbor discovery and route computation process. The neighbor nodes reply with the available path to the source node and the path which has minimum hops and less energy overhead will be selected as the path to reach the base station. The adversary node reply with small hop count and as it has direct connection to the base station and it is the only shortest route to reach the destination. By seeing this, the source node starts transmitting through the adversary node, which may discard the packet or perform modification attacks.

Identifying sinkhole present in the wireless sensor network is the key problem here and performed in many ways in the literature. The location of sinkhole can be performed using the location of the nodes and location verification can be done. Sinkhole attack threatens the security of WSNs at almost every layer of their protocol stack. The main deception of the attack is that a malicious node attracts the traffic of its neighbors by pretending that it has the shortest path to the base-station. The attack may jeopardize many important security measures.

In this study, we propose a quadratic approach to find the presence of sinkhole and mitigation of sinkhole attack. Our contribution is summarized as follows:

- First neighbor energy holes are used to find out the sinkhole attacks
- A centralized sinkhole attack detection model is proposed here

Corresponding Author: R. Murugesan, Department of ECE, Ultra College of Engineering and Technology for Women, 625104 Madurai, India

- The overhead of performing sinkhole monitoring in distributed manner is reduced by employing centralized approach here
- We propose light weight verification method to eliminate sinkholes

Literature review: There are many approaches has been proposed in the literature for sinkhole detection, we explore few of them here according to our problem statement. Efficient hole detour scheme for geographic routing in wireless sensor networks (Yu *et al*., 2008), consumes more energy of the nodes on the boundary of the hole, thus possibly enlarging the hole, we call this hole diffusion problem; on the other hand, it may incur data congestion if multiple communication sessions are bypassing the hole simultaneously. In this study, we propose efficient hole detour scheme to solve the hole problems faced by geographic routing in wireless sensor networks. Simulation results show that the proposed protocol is superior to other protocols in terms of packet deliver ratio, control overhead, average delivery delay and energy consumption.

By passing hole scheme using observer packets for geographic routing in WSNs (Choi and Choo, 2011), propose BHOP-GR (By passing Hole Scheme Using Observer Packets for Geographic Routing) that selects the optimum bypassing path while minimizing overhead to maintain hole boundary information. Several schemes have been recently proposed to solve this problem. However, they have overhead about nodes that are adjacent to the hole that have to maintain hole boundary information and increase hop count due to additional data packet transmission. BHOP-GR detects the hole boundary using an observer packet previously. When it transmits the data packet using a time delay, this can be arranged to decrease the average hop counts and routing path length. Also, using a virtual regular hexagon model which can exactly cover a hole to be detoured, minimizes overhead to maintain hole boundary information. In the performance evaluation, we show that BHOP-GR has at least 34 and 25% of the average hop counts and routing path length compared to SLGF (Safety Information based Limited Geographic greedy Forwarding) and virtual circle, respectively.

Virtual convex polygon based hole boundary detection and time delay based hole detour scheme in WSNs (Shin *et al*., 2009), propose a novel virtual convex polygon based hole boundary detection and time delay based hole detour scheme. The proposed scheme solves first and second hole diffusion problems.

Detection of wormhole attacks in wireless sensor networks using range-free localization (Otero and Hernandez, 2012), propose two wormhole detection procedures for WSNs, based on concepts employed in a kind of range-free localization methods: one of the approaches performs the detection simultaneously with the localization procedure and the other operates after the conclusion of the location discovery protocol. Both strategies are effective in detecting wormhole attacks but their performance is fairly sensitive to shadowing effects present in the radio channels.

SeRA: A secure routing algorithm against sinkhole attacks for mobile wireless sensor networks (Teng and Zhang, 2010), present a secure routing algorithm against sinkholes attacks based on mobile agents designed for Mobile Wireless Sensor Networks (MWSN) and show how it can be configured to avoid sinkhole attacks. Detection and correction of sinkhole attack with Novel method in WSN Using NS2 Tool, uses a sequence number based sinkhole detection approach. The sender node first requests the sequence number with the rreq message, if the node replies its sequence number with rrep message. Transmitting node will match sequence number in its routing table. If matches then data will be shared otherwise it will be assign the sequence number to the node. If the node accepts the sequence number then the node will enter in the network otherwise it will be eradicated from the network.

Detection of sinkhole attack in wireless sensor networks (Krontiris *et al*., 2008) proposes a Sybil attack detection scheme which initially uses the consistency of data to find the group of suspected nodes. Then, the intruder is recognized efficiently in the group by checking the network flow information. The proposed algorithm's performance has been evaluated by using numerical analysis and simulations. Therefore, accuracy and efficiency of algorithm would be verified.

Intrusion detection of sinkhole attacks in large-scale wireless sensor networks, proposes a novel algorithm for detecting sinkhole attacks for large-scale wireless sensor networks. We formulate the detection problem as a change-point detection problem. Specifically, we monitor the CPU usage of each sensor node and analyze the consistency of the CPU usage. Thus, the proposed algorithm is able to differentiate between the malicious and the legitimate nodes. A sinkhole attack detection scheme in mintroute wireless sensor networks (Rassam *et al*., 2012), where the vulnerabilities of mintroute protocol to sinkhole attacks are discussed and the existing manual rules used for detection are investigated using different architecture.

Detection and defence of Sinkhole attack in Wireless Sensor Network (Qi *et al*., 2012), realizes a mechanism to launch sinkhole attack at wireless sensor networks. And then, we present some mechanisms to detect and defense this type of attack. Finally, we do some experiments to verify our methods. Secure neighbor discovery in wireless sensor networks using range-free localization techniques present a framework generically called Detection of Wormhole Attacks using Range-Free methods (DWARF) under which we derive two specific wormhole detection schemes: the first approach, DWARF Loc, performs jointly the detection and localization procedures employing range-free techniques, while the other, DWARF test, uses a range-free method to check the validity of the estimated position of a node once the location discovery protocol is finished. Simulations show that both strategies are effective in detecting wormhole attacks and their performances are compared with that of a conventional Likelihood Ratio Test (LRT).

A non cryptographic method of sinkhole attack detection in wireless sensor networks (Sheela *et al*., 2011), proposed scheme to defend against sink hole attacks using mobile agents. 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 an effective paradigm for distributed applications and especially attractive in a dynamic network environment. A routing algorithm with multiple constraints is proposed based on mobile agents. It uses mobile agents to collect information of all mobile sensor nodes to make every node aware of the entire network, so that a valid node will not listen the cheating information from malicious or compromised node which leads to sink hole attack. The significant feature of the proposed mechanism is that it does not need any encryption or decryption mechanism to detect the sink hole attack. This mechanism does not require more energy than normal routing protocols like AODV. Here, we implement a simulation-based model of our solution to recover from a sinkhole attack in a wireless sensor network. The mobile agents were developed using the aglet.

In detection of sinkhole attack in wireless sensor networks using message digest algorithms (Sharmila and Umamaheswari, 2011), the proposed method destination/sink detects the attack only when the digest obtained from the trustable forward path and the digest obtained through the trustable node to the destination are different. It also ensures the data integrity of the messages transferred using the trustable path. The algorithm is also robust to deal with cooperative malicious nodes that attempt to hide the real intruder. The functionality of the proposed algorithm is tested in MAT lab.

A non cryptographic method of sinkhole attack detection in wireless sensor networks (Kuldeep and Mahadevan, 2014). We propose a region based sinkhole detection approaches which work using the neighbor conditions for the development of quality of service in wireless sensor networks.

MATERIALS AND METHODS

Sinkhole monitoring: The base station maintains neighbor details which has location information's about the neighboring nodes. With the neighbor details, the base station monitors the data flow from each of the neighbor and their signal strength and number of packets being received at each time frame. At each time window T_w, the base station BS computes number of packets Np, being received from each of the neighbor N_i and their possible residual energy N_e. We compute the energy flow factor Ef which shows the fraction of energy loss occurred at each time frame or time window for each of the neighbor. Based on computed Energy flow factor, we select set of neighbor nodes for sinkhole detection process. The number of packets being received from node N_i can be computed using the following Eq. 1:

$$NP_{TW} = \sum_{1}^{N} Rec(N_i) \tag{1}$$

Equation 1 shows the number of packets being received by any single node N_i at each time window Tw. The energy depletion occurred at each neighbor of base station is computed using the following Eq. 2:

$$EF_{TW} = \sum_{1}^{N} (\mu \times Pl) \tag{2}$$

Where:

μ = Energy source constant for each byte
Pl = Payload of the packet

RESULTS AND DISCUSSION

Region based sinkhole detection: The region based approach combines both centralized and distributed behavior of sinkhole detection. The base station selects and identifies the possible region from computed neighbors for the sinkhole detection process. The geographic region of the base station is divided into four quadratic regions of angles 90°. For each of the quadratic region the presence of guilty neighbor is identified, if there is any possible neighbor present in the computed

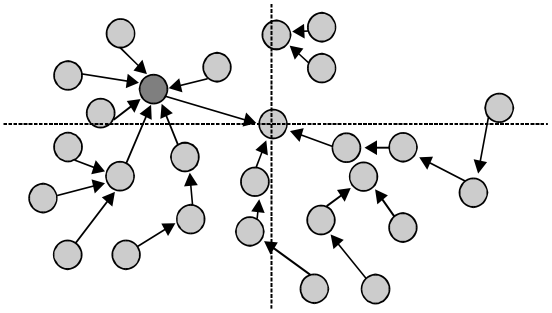

Fig. 1: Example snapshot of network

possible neighbors with energy flow fraction and then the region will be selected for sinkhole detection. The base station sends a one hop neighbor discovery command to the nodes of the selected quadratic region. Upon receiving this neighbor discovery command, the node will perform one hop neighbor discovery which collects neighbor information's from its neighbors and send to the base station. By receiving this reply, the base station verifies the truthiness of neighborhood from the location details of the nodes which has already. The base station computes original neighbor nodes for each of the nodes of the network and identifies available paths. From computed trustworthy of neighbor nodes the base station identifies the node which is present in most of the nodes neighbor table and which performs sinkhole attack (Alogrithm A).

Figure 1 shows the network which is split into four different region. The protocol performs sink hole detection at each region.

Algorithm A; neighbour nodes:

```
Step1: start
Step2: initialize quadratic regions qr, initialize guilty neighbors Gn, Sink set Sn.
Step3: Read Neighbor table Nt, Energy depletion matrix computed EF, location details LD.
Step4:  for each quadratic region $Qr_i$
                Identify depletion neighbors DN = $Ø(EF_{tw})$.
    compute one hop neighbor discovery ND = {seq.No, Node.ID, Base.ID, OHND}.
                for each neighbor $Nr_i$ from DN
                        send ND.
                end.
    end
Step5: receive OHND-Reply from neighbors $N_i$ from DN.
Step6: for each node $N_i$ from Qr
                Identify Common Neighbors CN.

                $CN = \int_{1}^{size(Qr)} Ni \in Nr(Ni)$
    $N_i$ – The common node as neighbor present in all nodes neighbor list.
    Nr – Neighbor list of Node N.
    perform location verification and topology statistics.
    $L_{Ni} = \Pi(Nr, LD)$.
    if $L_{Ni}$ = False then
                add to Sn = $sn+N_i$.
    End.
End
step7: Stop.
```

Mitigation of sinkhole attacks: The base station computes an alert message, which has information and location of sinkhole or adversary node and send to the neighbors from the region. On the other hand, the neighbor node will multicast to its neighbors other than sinkhole node. Finally, this alert message will be flooded into the sub-network and reach all the nodes present in the geographic region of the network. Here after, the nodes will compute path, which does not pass through the sinkhole node (Alogrithm B).

Algorithm B; sinkhole node:

```
Step1: Start
Step2: Read neighbor matrix N, sinkhole Sn.
Step3: Compute sink alert message SA.
    SA = {Seq.ID, Node.ID, BaseID, SinkAddress Sn}.
Step4: Broadcast SA.
Step5: Receive packet P.
            if P.Type = SA
                    Sn = SA.SN.
                    Nt = $\Pi(Sn \times Nt)$.
                    Broadcast SA.
            End.
Step6: Stop.
```

Experimental analysis: The proposed neighbor condition based sinkhole detection approach has been implemented in Network Simulator NS2. We have designed network topology with different scenarios with different number of nodes. The proposed methodology has been evaluated with different density networks with multiple sinkhole nodes. Table 1 shows the simulation parameters used to evaluate the proposed method. NS-2 has written using C++ language and it uses Object Oriented Tool Command Language (OTCL). It came as an extension of Tool Command Language (TCL). The simulations were carried out using a WSN environment consisting of 71 wireless nodes over a simulation area of 1000×1000 m flat space operating for 60 sec of simulation time. The radio and IEEE 802.11 MAC layer models were used.

The overhead generated by sinkhole detection process has been shown in Fig. 2. It shows that the proposed approach has produced less overhead than other methods while performing sinkhole detection process.

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 (Table 2).

Figure 3 hows the overall throughput ratio of different methods and it is clear that the proposed NCBSD method has achieved higher throughput than other methods.

Table 1: The parameters used in our simulation

Parameters	Value
Version	NS-allinone 2.28
Protocols	NCSD
Area	1000×1000 m
Transmission range	250 m
Traffic model	UDP,CBR
Packet size	512 bytes

Table 2: Shows the comparison results

		Detection rate			

Number of nodes	Protocol	False +ve	False -ve	Throughput	PDF
71	Geostatical Hazard model	3.5	2.5	92	86.70
71	NCSD	0.9	0.8	97.8	93.50

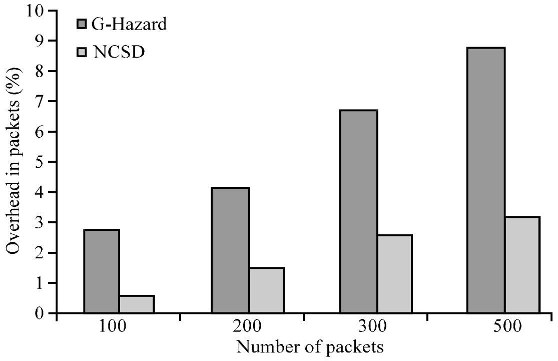

Fig. 2: Shows the overhead generated by sinkhole detection

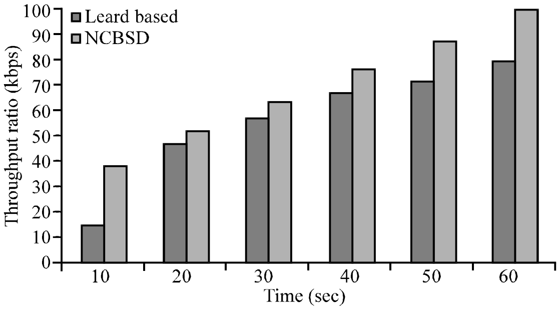

Fig. 3: Hroughput ratio of different methods

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 ratio (PDF) is computed as follows:

$$\text{PDF} = \left(\frac{\text{No.of packets received}}{\text{No.of packet sent}}\right) \times 100$$

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

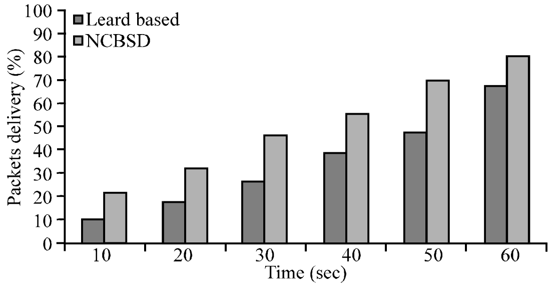

Fig. 4: Packet delivery ratio

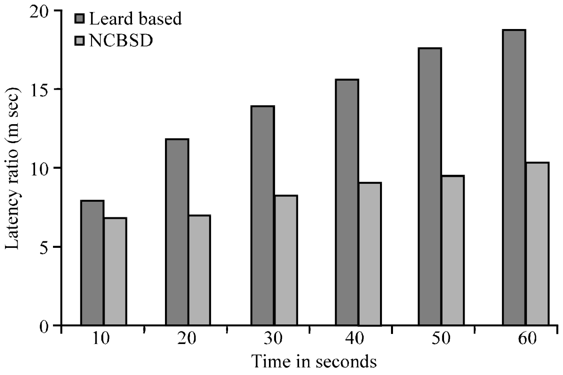

Fig. 5: End-to-end delay

Average end-to-end delay: Average end to end delay includes all possible delay caused by buffering during route discovery latency, queuing at the interface queue and delay at the MAC due to retransmission, propagation and transfer time. It is defined as the time taken for a data packet to be transmitted across a MANET from source to destination.

$$\text{Delay} = t_R - t_s$$

Where:

t_R = The receiving time and
t_S = Is the sent time

Figure 5 shows the latency ratio of different methods and it shows clearly that the proposed method has lower latency ratio than others.

CONCLUSION

The base station maintains location information about all the nodes present under the coverage and it performs sinkhole detection process periodically. It computes number of packets received at each time window from its neighbor to identify the presence of sinkhole at any of the quadratic region of its geographic coverage. If any of the regions is suspected to sinkhole attack it starts detection process at that particular region only. The neighbor nodes and other nodes from the quadratic region helps finding the adversary node and intimated by an alert message showing that there is an adversary which has to be avoided at future transmissions. The proposed method has reduced the overhead generated by distributed sinkhole detection process and produced efficient results.

REFERENCES

Choi, M. and H. Choo, 2011. Bypassing hole scheme using observer packets for geographic routing in WSNs. Proceeding of the 2011 International Conference on Information Networking (ICOIN), January 26-28, 2011, IEEE, Barcelona, Spain, pp: 435-440.

Krontiris, I., T. Giannetsos and T. Dimitriou, 2008. Launching a sinkhole attack in wireless sensor networks; the intruder side. Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2008, WIMOB'08, October 12-14, 2008, IEEE, Avignon, France, pp: 526-531.

Otero, G.M. and A.P. Hernandez, 2012. Detection of wormhole attacks in wireless sensor networks using range-free localization. Proceeding of the 2012 IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), September 17-19, 2012, IEEE, Barcelona, Spain, pp: 21-25.

Qi, J., T. Hong, K. Xiaohui and L. Qiang, 2012. Detection and defence of sinkhole attack in wireless sensor network. Proceedings of the IEEE 14th International Conference on Communication Technology, November 9-11, 2012, Chengdu, pp: 809-813.

Rassam, M.A., A. Zainal, M.A. Maarof and M. Al-Shaboti, 2012. A sinkhole attack detection scheme in mintroute wireless sensor networks. Proceeding of the 2012 International Symposium on Telecommunication Technologies (ISTT), November 26-28, 2012, IEEE, Kuala Lumpur, pp: 71-75.

Sharmila, S. and G. Umamaheswari, 2011. Detection of sinkhole attack in wireless sensor networks using message digest algorithms. Proceeding of the 2011 International Conference on Process Automation, Control and Computing (PACC), July 20-22, 2011, IEEE, Coimbatore, India, pp: 1-6.

Sheela, D., K.C. Naveen and G. Mahadevan, 2011. A non cryptographic method of sinkhole attack detection in wireless sensor networks. Proceedings of the IEEE International Conference on Recent Trends in Information Technology, June 3-5, 2011, Chennai, Tamil Nadu, pp: 527-532.

Shin, I., N.D. Pham and H. Choo, 2009. 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. Michael, S.J. and S. Gavriel (Eds.). Springer Berlin Heidelberg, Heidelberg, Germany, pp: 619-627.

Teng, L. and Y. Zhang, 2010. SeRA: A secure routing algorithm against sinkhole attacks for mobile wireless sensor networks. Proceedings of the 2nd International Conference on Computer Modeling and Simulation, Volume 4, January 22-24, 2010, Sanya, Hainan, pp: 79-82.

Yu, F., S. Park, Y. Tian, M. Jin and S.H. Kim, 2008. Efficient hole detour scheme for geographic routing in wireless sensor networks. Proceeding of the Vehicular Technology Conference on VTC Spring 2008, May 11-14, 2008, IEEE, Singapore, Asia, pp: 153-157.