ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

Study on Sinkhole Attack Detection in Wireless AdHoc Networks

Thamayanthi.M[1], Jayashree.R[2], Priya.V[3], Sumathi.M[4]

Student, Computer Science and Engineering, St.Joseph's College of Engineering and Technology, Thanjavur, India[1,2,3]

Student, Network Engineering, Kalasalingam University, Virudhunagar, India[4]

Abstract—Wireless ad hoc network is a collection of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. As compared to conventional network, wireless ad hoc network are more vulnerable to the security attacks. The nature and structure of wireless ad hoc network makes it very attractive to attackers, because there is no fixed infrastructure and administrative approach in it. "Sinkhole attack" is one of the severe attacks in this type of network; this makes trustable nodes to malicious nodes that result in loss of secure information. This paper focuses on sinkhole attacks on routing protocols such as DSR, AODV. To overcome the problems occur due to sinkhole we discuss about Security-aware routing (SAR) which helps to reduce the impact of such attack.

Keywords—DSR, AODV, SAR, Sinkhole attack, geographic routing, MANET.

I.INTRODUCTION

Wireless Ad hoc Network consists of autonomous mobile nodes interconnected by wireless multi hop communication paths. They can communicate and move at the same time. Wireless Adhoc networks have no fixed network infrastructure or administrative support, unlike other conventional network that requires fixed network infrastructure. Mobile ad hoc networks, MANET have its significancy by multihop and infrastructureless data transmission. High mobility of node make the traditional routing protocols(DSDV,AODV,DSR) susceptibile and not suitable for large scale networks. These algorithm require predetermination of end to end routing. Since it is mobile networks, predetermination of end to end are not possible to found. If there is any path breakage,the data either lost or there may be delay at the destination. Geographic information makes use of the location information of the nearby nodes.

If the location information is inaccurate then it is not effective. In Greedy forwarding,the forwarder node is the node far away from the source.Any of the node is out of the coverage range then the node is not reachable and the transmission gets failed.In GPSR,a famous GR protocol MAC failure feedback is send to the to the forwarder node thereby the packet is rerouted and data is received at the destination. General problem in data transmission is that single transmission of packet leads to multiple reception due to interruption,traffic,etc. Location based POR has been proposed now. Itdirectly uses location information for guiding packet forwarding. Like other opportunistic routing protocols, it is designed for static mesh networks and focuses on network throughput.. If the best forwarder does not forward the packet in certain time slots, suboptimal candidates will take turn to forward the packet according to a locally formed order. The data transmission will not be interrupted if the candidates succeeds in receiving and forwarding the packets. Duplicate relaying is important fact to be considered in forwarding packets in node mobility and in collision.

II. SINKHOLE ATTACK

A. Overview

Sinkhole attack is one of the severe attacks in wireless Ad hoc network. In sinkhole Attack, 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 neighboring 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 . In this way the path presented through the malicious node appears to be the best available route for the nodes to communicate. In DSR protocol, sinkhole attack modifies sequence no in RREQ.Due to the destination node's movement, the multihop path may diverge from the true location of the final destination and a packet would be dropped even if it has already been delivered into the neighborhood of the destination. To deal with such issue, additional check for the destination node is introduced. At each hop, the node the MAC multicast mode. The use of RTS/CTS/DATA/ACK significantly reduces the collision and all the nodes within the transmission range of the sender can eavesdrop on the packet successfully with higher probability. The basic routing scenario of POR can be simply illustrated in Fig. 1. In normal situation without link break, the packet is forwarded by the next hop node (e.g., nodes A, E) and the forwarding candidates (e.g., nodes B, C; nodes F, G) will be suppressed (i.e., the same packet in the Packet List will be dropped) by the next hop node's transmission. In case node A fails to deliver the packet (e.g., node A has moved out and cannot receive the packet), node B, the forwarding candidate with the highest priority, will relay the packet and suppress the lower priority candidate's forwarding (e.g., node C) as well as node S.For the packet pulled back from the MAC layer,itwill not be rerouted as long as node S overhears node B'sforwarding.

B. Selecting forwarding candidates

One of the key problems in POR is the selection and prioritization of forwarding candidates.The forwarding area is determined by the sender and the next hop node. A node located in the forwarding area satisfies the following two conditions:
1) it makes positive progress toward the destination; and
2) its distance to the next hop node should not exceed half of the transmission range of a wireless node (i.e., R/2) so that ideally all the forwarding candidates can hear from one another. In Fig. 1, the area enclosed by the bold curve is defined as the forwarding area. The nodes in this area, besides node A (i.e., nodes B, C), are potential candidates. The priority of a forwarding candidate is decided by its distance to the destination. The nearer it is to the destination, the higher priority it will get. When a node sends or forwards a packet, it selects the next hop forwarder as well as the forwarding candidates among its neighbors. The next hop and the candidate list comprise the forwarder list. Algorithm 1 shows the procedure to select and prioritize the forwarder list.

```
Algorithm 1.Candidate Selection
ListN : Neighbor List
ListC : Candidate List, initialized as an empty list
ND    : Destination Node
Base : Distance between current node and ND
if  find(ListN,ND) then
    next_hop←ND
    return
end if
fori← 0 to length(ListN) do
    ListN[i].dist←dist(ListN[i],ND)
end for
ListN.sort()
next_hop←ListN[0]
fori←1 to length(ListN) do
    if  dist(ListN[i],ND)>=base or length(ListC)=N
    then
        break
    else if dist(listN[i],listN[0])<R/2 then
        ListC.add(ListN[i])
    end if
end for
```

Every node maintains a forwarding table for the packets of each flow (identified as source-destination pair) that it has sent or forwarded. Before calculating a new forwarder list, it looks up the forwarding table to check if a valid item for that destination is still available. The forwarding table is constructed during data packet transmissions and its maintenance is much easier than a routing table.It depends on the local information and takes less time to construct. Forwarding table records the active flow only.

C. Limitation on Possible Duplicate Relaying

Some forwarding candidates may fail to receive the packet due to the high mobility and collision.If the next forwarding candidate also follows the same,then the propagation area increases with destination as centre andradius can be as large as the distance between the source and the destination. To limit suchduplicate relaying, the packet that has been forwardedby the source and the next hop node is transmitted by opportunistic fashion and is allowed to be cached by multiple candidates.Here instead of allowing the packets to be cached by many candidates, it can be made more effective by forwarding only to the next hop and the very next priority node.Only the source and the next hop node need to calculate the candidate list, while for the packet relayed by a forwarding candidate, the candidate list is empty.The propagation area of a packet is limited to a certain band between the source and thedestination, as illustrated in Fig. 2.

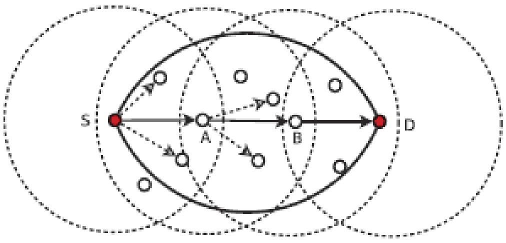

Fig. 2. Duplicate relaying is limited in the region enclosed by the bold curve.

III. ROUTE PHASE

A.MAC Interception

In the network,some alteration on the packet transmission scenario is made.Just send the packet via unicast, to the best node which is elected by greedy forwarding as the next hop. In this way, we make full utilization of the collision avoidance supported by 802.11 MAC. While on the receiver side, we do some modification of the MAC-layer address filter: even when the data packet's next hop is not the receiver, it is also delivered to the upper layer but with some hint set in the packet header indicating that this packet is overheard. It is then further processed by POR. Hence, the benefit of both broadcast and unicast (MAC support) can be achieved.

As the location information of the neighbors is updated periodically, some items might become obsolete very quickly especially for nodes with high mobility. This scheme introduces a timely update which enables more packets to be delivered.

B. Interface Queue Inspection

The main point of POR is that when an intermediate node receives a packet with the same ID,having same source and sequence number then it will drop that packet from its packet list. Besides maintaining the packet list,we also check the interface queue.

IV. EFFECT OF SINKHOLE ATTACK

For better POR in void handling special mechanism should be proposed based on virtual destination.

A. Trigger Node

The main thing is which node should forward packet from greedy mode to void handling mode.The change happens at void node mostly. e.g., Node B in Fig. 3. Then, Path 1

(A-B-E---) and Path 2 (A-B-C-F---) (in some cases, only Path 1 is available if Node C is outside Node B’s transmission range) can be used to route around the communication hole.

From Fig. 3, it is obvious that Path 3 (A C-F---) is better than Path 2. If the mode switch is done at Node A, Path 3 will be tried instead of Path 2 while Path 1 still gets the chance to be used. A message called void warning, which is actually the data packet returned from Node B to Node A with some flag set in the packet header, is introduced to trigger the void handling mode. As soon as the void warning is received, Node A (referred to as trigger node) will switch the packet delivery from greedy mode to void handling mode and rechoose better next hops to forward the packet. node will give up trying the other direction. For the same flow, the path acknowledgment will be periodically sent.

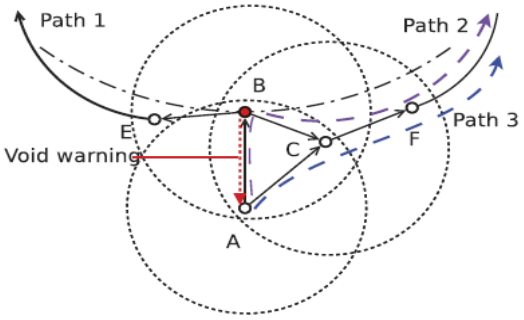

Fig. 3.Potential paths around the void.

On the other hand, if a packet that is forwarded in voidhandling mode cannot go any further or the number of hopstraversed exceeds a certain threshold but it is still being delivered in void handling mode, a DISRUPT control packet will be sent back to the trigger node as reverse suppression. Once the trigger node receives the message, it will stop trying that direction. Therefore, a scaling parameter is introduced for the candidates located in A-II. The progress toward the virtual destination made by these nodes is multiplied by a coefficient n(0<n< 1), called scaling parameter.

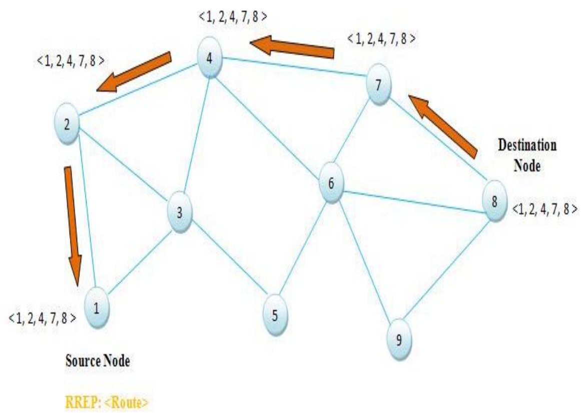

Fig. 4. Route Reply Propagation in DSR.

B. Virtual Destination

In order to enable opportunistic forwarding in void handling, which means even in dealing with voids, we can still transmit the packet in an opportunistic routing like fashion, virtual destination is introduced, as the temporarytarget that the packets are forwarded to. Virtual destinations are located at the circumference with the trigger node as center (Fig. 4), but the radius of the circle is set as a value that is large enough (e.g., the network diameter). They are used to guide the direction of packet delivery during void handling. Compared to the real destination D, a virtual destination (e.g., D0 left and D0 right) has a certain degree of offset in Fig. 4.

For those communication holes with very strange shape, a reposition scheme has been proposed to smooth the edge of the hole. Given the work that has been done in, VDVH thus still has the potential to deal with all kinds of communication voids. Fig. 5 shows an example in which VDVH achieves the optimal path of seven hops while GPSR undergoes a much longer route of 15 hops.

*1)Switch Back to Greedy Forwarding:*A fundamental issue in void handling is when and how to switch back to normal greedy forwarding. From Fig. 4 we can see that the forwarding area in void handling can be divided into two parts: A-I and A-II. To prevent the packet from deviating too far from the right direction or even missing the chance to switch back to normal greedy forwarding, the candidates in A-I should be preferred and are thus assigned with a higher priority in relaying.

*2) Path Acknowledgment and Disrupt Message:*In VDVH, if a trigger node finds that there are forwardingcandidates in both directions, the data flow will be split intotwo where the two directions will be tried simultaneouslyaround the communication void. Path acknowledgment and reverse suppression are introduced. Once the packet reaches the destination, a path acknowledgment will be sent along the reverse path to inform the trigger node. Then, the trigger

V. MEMORY CONSUMPTION AND DUPLICATE RELAYING

One main concern of POR is its overhead due toopportunistic forwarding, as several copies of a packet need to be cached in the forwarding candidates, leading to more memory consumption, and duplicate relaying would possibly happen if the suppression scheme fails due to node mobility.In memory consumption if a packet is received by a forwarding candidate C, it will be cached for a period of I Δtat most according to the forwarding scheme. we can get the following upper bound for the length (number of packets cached) of the packet list Qi at Ci for each flow:

$$Q_i \leq r_s.i\Delta T$$

whereas is the packet sending rate at the source of the dataflow. Suppose rs=100 packets/s (which is relatively heavy traffic); since we have set T=0:01 s, Qi would not exceed i, indicating that the opportunistic forwarding scheme used in our protocol will not consume much memory resource.

A. No Forwarding Candidate Is Involved(N=0)

In this case there are two possible cases: 1) the packet sent from S is successfully received by C0, so it is forwarded only once; and 2) C0 fails to receive the packet (i.e., it has moved out), then S reselects another next hop for this packet, and thus the packet is forwarded twice at this hop.

B. One Forwarding Candidate Is Involved(N=1)

Here the source of duplication is not only S's rerouting, but also C1's duplicate relaying due to its moving out (i.e., C1 is no longer within C0's transmission range but is still within S's transmission range)

C. Two Forwarding Candidates Are Involved(N=2)

When two forwarding candidates are involved, we have to take duplicate relaying into more consideration. Though C1 and C2 will be suppressed by C0 with high probability, in the case that C0 moves out and C1 forwards the packet instead, C2 may not be successfully suppressed (as illustrated in Fig. 6b) since the initialized distance between C1 and C2 can be as far as R and they are much more likely to get separated (i.e., being outside each other's transmission range).

- Packet delivery ratio: The ratio of the number of data packets received at the destination(s) to the number of data packets sent by the source(s).
- End-to-end delay : The average and the median end-to end delay are evaluated, together with the cumulative distribution function of the delay.
- Path length : The average end-to-end path length(number of hops) for successful packet delivery.
- Packet forwarding times per hop (FTH): The average number of times a packet is being forwarded from the perspective of routing layer to deliver a data packet over each hop.
- Packet forwarding times per packet (FTP): The average number of times a packet is being forwarded from the perspective of routing layer to deliver a data packet from the source to the destination.

Among the metrics, FTH and FTP are designed to evaluate the amount of duplicate forwarding. For unicast style routing protocols, packet reroute caused by path break accounts for FTH being greater than 1. On the other hand, for those packets who fail to be delivered to the destination(s), the efforts that have already been made in forwarding the packets are still considered in the calculation of FTH, as FTH is calculated as follows:

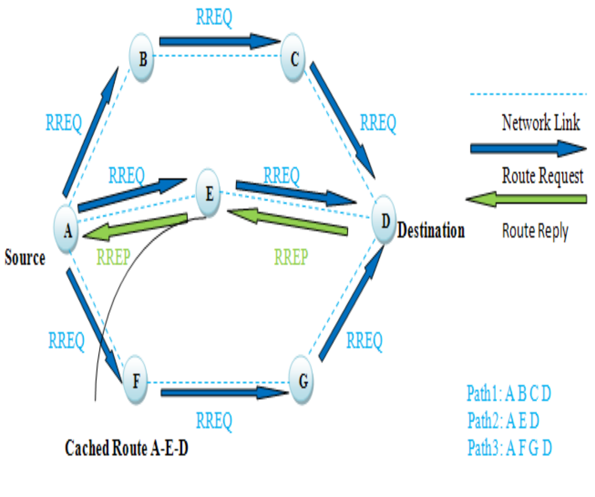

Fig.5 A possible path for a route replies if A wishes to find a route to D

$$\text{FTP}=\frac{N_s+N_f}{\sum_{i=0}^{Nr} N_{hi}}$$

where N_s, N_f , and N_r are the number of packets sent at thesource(s), forwarded at intermediate nodes, and received atthe destination(s), respectively. N_{hi} is the number of hopsfor the ith packet that is successfully delivered.FTP averages the total number of times a packet is beingforwarded on a per-packet basis:

$$\text{FTP}=\frac{N_s+N_f}{N_r}$$

To prevent the packet from deviating too far from the right direction or even missing the chance to switch back to rmal greedy forwarding, the candidates in A-I should be preferred and are thus assigned with a higher priority in relaying. Therefore, a scaling parameter is introduced for the candidates located in A-II.

VI. Communication Hole Effectiveness

To test the effectiveness of VDVH, we further evaluate therouting performance in mobile networks with a communicationhole. We create a network topology Thesource and destination nodes are fixed at the two ends of the rectangle while the remaining nodes moves randomly. The central gray area is simulated as the communication hole with no mobile node distributed. By changing the maximum node speed, we obtain the simulation results. we can observe that in the face of communication hole, GPSR's void handling mechanism fails to work well. Even when the maximum node speed is 5 m/s, only 90 percent of the data packets get delivered which is relatively poor compared to the other protocols. However, when the node mobility is high (e.g., when the maximum node speed is larger than 25 m/s), POR still performs better. As a summary, POR outperforms AOMDV and GPSR in packet delivery ratio, end-to-end delay, as well as resource (bandwidth) efficiency.

VII. Related Work

Existing robust routing protocols for MANETs can be classified into two categories. One uses the end-to-end redundancy, e.g., multipath routing, while the other leverages on the hop-by-hop redundancy which takes advantage of the broadcast nature of wireless medium and transmits the packets in an opportunistic or cooperative way. Our scheme falls into the second category.Multipath routing, which is typically proposed to increase the reliability of data transmission in wireless ad hoc networks, allows the establishment of multiple paths between the source and the destination.

In the existing protocols, if the failure time exceeds a certain threshold, the guard node who has recently accomplished the forwarding will become the new intended node. A potential problem is that such substitution scheme may lead to suboptimal paths. Unlike RRP, our protocol uses location information to guide the data flow and can always archive near optimal path. On the other hand, our scheme focuses on the route discovery from the perspective of network layer and no such complex MAC modification is necessary.

VII. CONCLUSION

In this paper, we address the problem of reliable data delivery in highly dynamic mobile ad hoc networks. Constantly changing network topology makes conventional ad hoc routing protocols incapable of providing satisfactory performance. frequent link break due to node mobility, substantial data packets would either get lost, or experience higher priority forwarder makes effective in time and reduces traffic and collision. The security of wireless ad hoc network can be enhanced by using different approach such as Security-aware routing (SAR) which applicable in both DSR and AODV routing protocols. As future work, we will try to implement one of indicator to detect sinkhole attack in network.

REFERENCES

[1] J. Broch, D.A. Maltz, D.B. Johnson, Y.-C.Hu, and J. Jetcheva, "APerformance Comparison of Multi-Hop Wireless Ad Hoc NetworkRouting Protocols," Proc. ACM MobiCom, pp. 85-97, 1998.

[2] M. Mauve, A. Widmer, and H. Hartenstein, "A Survey onPosition-Based Routing in Mobile Ad Hoc Networks,"IEEENetwork, vol. 15, no. 6, pp. 30-39, Nov./Dec. 2001.

[3] D. Chen and P. Varshney, "A Survey of VoidHandlingTechniques for Geographic Routing in Wireless Networks," IEEEComm. Surveys and Tutorials, vol. 9, no. 1, pp. 50-67, Jan.-Mar. 2007.

[4] D. Son, A. Helmy, and B. Krishnamachari, "The Effect of MobilityInduced Location Errors on Geographic Routing in Mobile AdHoc Sensor Networks: Analysis and Improvement Using MobilityPrediction," IEEE Trans. Mobile Computing, vol. 3, no. 3, pp. 233- 245, July/Aug. 2004.

[5] B. Karp and H.T. Kung, "GPSR: Greedy Perimeter StatelessRouting for Wireless Networks," Proc. ACM MobiCom, pp. 243-254, 2000.

[6] S. Biswas and R. Morris, "EXOR: Opportunistic Multi Hop Routingfor Wireless Networks," Proc. ACM SIGCOMM, pp. 133-144, 2005.

[7] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "TradingStructure for Randomness in Wireless Opportunistic Routing,"Proc. ACM SIGCOMM, pp. 169 180, 2007.

[8] E. Rozner, J. Seshadri, Y. Mehta, and L. Qiu, "SOAR: SimpleOpportunistic Adaptive Routing Protocol for Wireless MeshNetworks," IEEE Trans. Mobile Computing, vol. 8, no. 12,pp. 1622-1635, Dec. 2009.

[9] A. Balasubramanian, R. Mahajan, A. Venkataramani, B.N. Levine,and J. Zahorjan, "Interactive WiFi
Connectivity for MovingVehicles," Proc. ACM SIGCOMM, pp. 427-438, 2008.

[10] K. Zeng, Z. Yang, and W. Lou, "Location-Aided OpportunisticForwarding in Multirate and MultihopWireless Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 6, pp. 3032-3040, July 2009.

[11] S. Das, H. Pucha, and Y. Hu, "Performance Comparison ofScalable Location Services for Geographic Ad Hoc Routing," Proc.IEEE INFOCOM, vol. 2, pp. 1228-1239, Mar. 2005.

[12] R. Flury and R. Wattenhofer, "MLS: An Efficient Location Servicefor Mobile Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 226-237, 2006.

[13] E. Felemban, C.-G.Lee, E. Ekici, R. Boder, and S.Vural,"Probabilistic QoS Guarantee in Reliability and TimelinessDomains in Wireless Sensor Networks," Proc. IEEE INFOCOM,pp. 2646-2657, 2005.

[14] D. Chen, J. Deng, and P. Varshney, "Selection of a ForwardingArea for Contention-Based Geographic Forwarding in WirelessMulti-Hop Networks," IEEE Trans