A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks

Kisung Kim and Sehun Kim
Department of Industiral Engineering, Korea Advanced Institute of Science and Technology,
373-1, Guseong-Dong, Yuseong-Gu, Daejeon, 305-701, Korea
Email:{kskim,shkim}@tmlab.kaist.ac.kr

Abstract

Mobile ad hoc network(MANET) is a kind of wireless network which has no infrastructure. Each component node of MANET can move freely and communicate based on wireless peer to peer mode. Because of its vulnerable routing protocols, MANET is exposed to many kinds of attacks. A sinkhole attack is one of the representative attacks in MANET caused by attempts to draw all network traffic to a sinkhole node. This paper focuses on the sinkhole problem on Dynamic Source Routing(DSR) protocol in MANET. To detect the sinkhole node, we extract several useful sinkhole indicators through analyzing the sinkhole problem, then propose an efficient detection method based on an incremental learning algorithm. The simulation results show that the proposed method is effective and reliable for detecting sinkhole intrusion.

1. Introduction

Mobile ad hoc network(MANET) is a wireless network which utilizes multi-hop radio relaying and is capable of operating without the support of any fixed infrastructure. The absence of fixed infrastructure that makes the routing decisions in centralized manner requires the MANET to route in distributed manner. This requires each component node of MANET to be more intelligent as a network router for routing packets from other nodes.

The nodes are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Because of its dynamic network topology, it is exposed to various network attacks including eavesdropping, selfish nodes, data tampering, network congestion etc. [1].

When a malicious which can modify the network routing packets or generate enormous artificial traffics takes part in the MANET, it makes network delay, energy consumption, finally makes the network disabled. Incumbent MANET routing protocols(AODV, DSR) are vulnerable to these attacks, so there are many researches to develop the defence algorithm against the attacks.

This paper analyzes one type of attack the 'sinkhole attack' that can easily be employed against MANET routing protocols. The sinkhole attack, a malicious node in MANET advertises a wrong routing information, such as advertising itself as being on the way to specific nodes, so receives the whole traffics in local network. Then it modifies the data packets or drops them to make the network complicated[2].

This paper focuses on detecting the sinkhole attacker on dynamic source routing (DSR) protocol effectively. By using sinkhole indicators a method based on incremental learning algorithm. Our study results provide an adaptive distributed sinkhole detector according to network situation.

The rest of the paper is organized as follows. In Sect.2, DSR protocol in MANET and related sinkhole attack are described. In Sect.3 the sinkhole indicators are introduced. In Sec.4 The proposed sinkhole detection algorithm is presented. In Sect.5 the performance of the proposed algorithm is presented. We make the conclusion and discuss the future work in Sec.6.

2. Research Background

2.1 Dynamic Source Routing Protocol

Routing protocols in MANET can be classified in to 'table-driven routing' and 'on-demand routing' protocols. Table-driven routing protocols are extensions of the wired network routing protocols. They keep the global routing information in each router, in form of table. Each time, the table is updated to maintain the correct information of network status. Since they maintain the route table, they can get the route to destination swiftly. However, they should keep the whole routing information and exchange routing information constantly to update the table.

On the other hand, on-demand routing protocols executes the path-finding process when a path is required by a node. Dynamic source routing protocol(DSR) is a representative on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks.

DSR protocol consists of route discovery phase and route maintenance phase. Mobile nodes get route information by initiating route discovery themselves, and by overhearing the route records in route request of other route discovery processes. They keep the route cache which contains source route, if new route is entered then update the cache. When a route path is broken, route error message is sent to the source node and reestablish the route in route maintenance phase.

In route discovery phase, any node can discover a route to other node in local ad hoc network. To get the route to the destination node, a node broadcasts a route request packet(RREQ) which contains a source id, destination id, sequence number. Each node receiving a RREQ, rebroadcasts the packet to its neighbors if it does not have a route to the destination in its cache. If it has, then it sends route reply packet(RREP) that contains the route information to the source node through reverse path of the RREQ

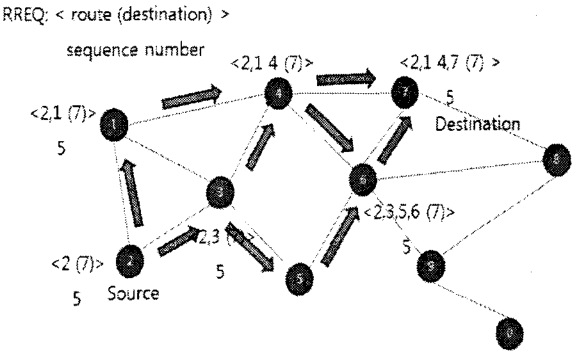


Figure 1. RREQ propagation

Figure 1 shows the RREQ propagation procedure. Node 5 broadcasts RREQ to its neighbors. Each intermediate node rebroadcasts the RREQ until the packet meets the destination node 7. Route < 2 1 4 7 > is selected and RREP is generated by node 7. RREP traverses through reverse route < 7 4 1 2 >. This procedure is well described in Figure 2.

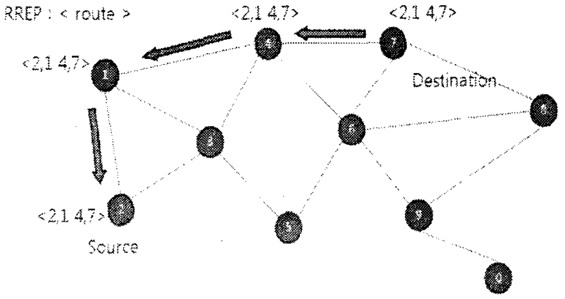


Figure 2. RREP propagation

When source node 2 received the RREP, it recognizes the route to the destination node 7. This is a route discovery phase, thereafter node 2 can send data packet through the received route.

2.2 Sinkhole Attack

Sinkhole attack, a sinkhole node tries to attract the data to itself from all neighboring nodes. It generates fake routing information that let the nodes in local network know itself on the way to specific nodes. Through this procedure, sinkhole node attempts to draw all network traffic to itself. Thereafter it alters the data packet or drops the packet silently. Sinkhole attack increases network overhead, decreases network's life time by boosting energy consumption, finally destroy the network[4].

In DSR protocol, sinkhole attack is set up by modifying sequence number in RREQ. Sequence number used to prevent loop formations indicates the recency of the route. The higher sequence number, the more recent route the packet contains. Sinkhole node selects the source, destination node. It observes the source node's sequence number carefully, and generates bogus RREQ with selected source, destination and higher sequence number than observed source sequence number. It adds itself on the source route and broadcasts the bogus RREQ. Nodes that take this bogus RREQ recognize that the reversed route could be a better route to the source than incumbent route.

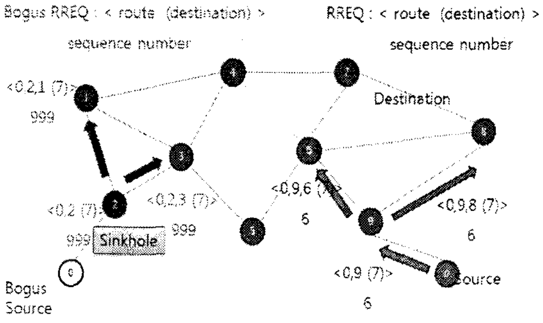


Figure 3. The generation of Bogus RREQ

Figure 3 shows the generation of the bogus RREQ packet. Sinkhole node 2 make the bogus RREQ which looks as if it is originated by node 0. Sequence number of bogus packet is 999, much higher than original source's, 6.

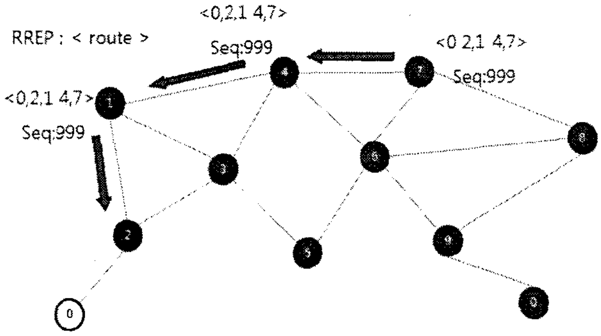


Figure 4. Bogus RREP propagation

Intermediate nodes on route learn that node 2 is on one hop distance to node 0 and to send packet to node 0, the data packet may go through the node 2. Sinkhole node 2 can easily repeat this procedure, draw all local network traffic to itself. Thereafter node 2 can do malicious acts including dropping, modifying the traffic.

3. Sinkhole Indicators.

Sinkhole Indicators are network features of occurrence of sinkhole attack on DSR protocol. Tseng et al proposed two sinkhole indicators, sequence number discontinuity, route add ratio. In this paper, Sequence number duplication is proposed as an indicator in addition to incumbent one.

3.1 Sequence number discontinuity

'Sequence number discontinuity (SeqN_D)' is a difference between source sequence number of current and last received RREQ. When a source node initiates route discovery, it publish sequence number, and increase its sequence number by 1. Because sinkhole node advertises fake route information by generating high sequence number, sequence number difference between normal and sinkhole node can be an clue of sinkhole's existence.

3.2 Route add ratio

Because of sinkhole node's advertising, nodes affected by fake route information include the sinkhole node in almost all of its route. So the proportion of route including sinkhole node to entire route in route cache become pretty high. This is what is called 'route add ratio (Ra_r)'. Through observing Ra_r it could be checked whether sinkhole node exist or not.

3.3 Sequence number duplicate

Bogus RREQ with large SeqN_D can last its effects for a long period. However it can also easily be detected by simple algorithm i.e.. if average SeqN_D is 20 then it is considered as a sinkhole attack. Therefore there could be more intelligent attack i.e.. make bogus packets with sequence numbers that are not unusually high. This kind of attack is called stealthier version of sinkhole attack. To detect stealthier version attack, a node can stores the source id, destination id and sequence number of each received or broadcasting RREQ. It doesn't require huge memory, but remembers several set of RREQ information.

In current DSR protocol, when a node received the RREQ, it checks sequence number to determine whether ignores the RREQ or not. If sequence number is not larger than last sequence number, then RREQ is dropped silently.

We propose that before drop the packet, identify the received RREQ. A detecting node finds the set of RREQ information where source id and sequence number is equal to those of received RREQ. If it is possible to find the specific RREQ, then check that the destination id of received RREQ and found RREQ are same. If they are not same, then the node recognizes the existence of sinkhole node.

4. Sinkhole Detection Algorithm

Sinkhole indicators are described in Sect 3. We develop an sinkhole detection algorithm using those indicators. Tseng et al presented the detection algorithm with SeqN_D and Ra_r. They suggested the constant threshold value for classifying the outlier, sinkhole node. This algorithm works very well for high sequence number attack, but does not for sequence number below the threshold. Sinkhole attack can produce various kind of sequence number and the network condition is changeable, therefore it is required to take the problem in statistical method to classify the normal and sinkhole status adaptively.

The network topology is highly flexible in MANET. Accordingly the use of a traditional static profile is not efficient[5]. Hence incremental learning based sinkhole detection algorithm is proposed to reflect the network's topology changes.

Each node observes the route message. When a node receive RREQ, SeqN_D, maximum Ra_r (MRa_r) are calculated. Let SeqN_D-i and MRa_r-i be the *ith* frame made of N SeqN_Ds, MRa_rs. After receiving N RREQ, the node calculates the average, standard deviation of SeqN_D, MRa_r of each frame.

$$aver(x^i) = \frac{1}{N}\sum_{k=1}^{N} x_k$$

$$std(x^i) = \frac{1}{N}\sum_{k=1}^{N}(aver(x^i) - x_k)^2$$

To reflect the trend of the network, A model consisting of an weighted average and std of M frames is proposed as follows.

$$aver(\bar{x}) = \frac{1}{N}\sum_{i=1}^{M}\lambda_i\, aver(x^i)$$

$$std(\bar{x}) = \frac{1}{N}\sum_{i=1}^{M}\lambda_i\, std(x^i)$$

where $\lambda_i = \lambda_0 \cdot \exp(-a \cdot i)$, $\sum_{i=1}^{M} \lambda_i = 1$

a is a constant parameter which controls the weighing factor λ. It is based on 'forgeting curve' algorithm[6]. A model fairly reflects M frames where a is zero. When a increases up to 1, the model gradually reflects a recent frame more than last frames.

Through this model, we can classifies outlier frame. Before recalculate the new $aver(\bar{x})$, $std(\bar{x})$, check incoming frame's $aver(x^i)$ is larger than incumbent $aver(\bar{x})$ plus $std(\bar{x})$. If $aver(x^i)$ is larger than $aver(\bar{x})+std(\bar{x})$, then the incoming frame is classified as an outlier. Because in case of sinkhole attack, SeqN_D and Ra_r are increasing rapidly, it is possible to consider this outlier as a clue of sinkhole attack.

If the frame is not considered as an outlier, then it is used to update the model by calculating new $aver(\bar{x})$ and $std(\bar{x})$. Else information from the frame is discarded and the detecting node is alarmed.

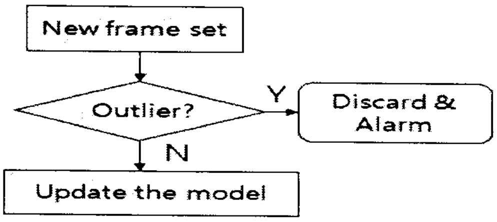


Figure. 5 Flowchart of proposed algorithm

A node detects the sinkhole existence by both SeqN_D and Ra_r alarm messages and finds the sinkhole node by MRa_r. A node which currently has maximum Ra_r is classified as sinkhole node. Thereafter, a node broadcasts alarm messages to other nodes to exclude the sinkhole node in their route.

There is another sinkhole indicator, sequence number duplicate. If sequence number duplicate is occurred in a detecting node, the node can recognize the sinkhole existence by Ra_r only. Because sequence number duplicate directly indicates the sinkhole existence and is occurred when sinkhole node trys to generate unusually high sequence number avoiding SeqN_D.

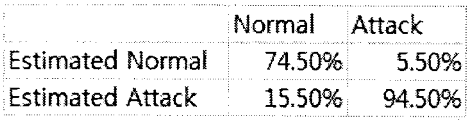
5. Simulations

In order to evaluate proposed detecting method, we experiment with network simulator, NS2. The simulation set up is as followings, figure 6.

Simulator	ns-2 (ver.2.31)
Simulation time	500s
Number of mobile nodes	50
Number of malicious node	1
Topology	670m x 670m
Routing Protocol	DSR
Maximum Bandwidth	2Mbps
Traffic	CBR
Maximum Connection	160
Maximum Speed	5(m/s)

Figure 6. Simulation parameter

Because there is no standard sinkhole attack, we develop the attack with modifying the sequence number. Figure 7 shows the detection rate according to attacks with a sequence number modification.



	Normal	Attack
Estimated Normal	74.50%	5.50%
Estimated Attack	15.50%	94.50%

Figure 7. Performance of the model with normal sequence number plus 10

Tseng et al suggested the 'SⅡS' method which is based on constant threshold acquired by their simulations[3]. The method didn't detect any attack whose SeqN_D is quite lower than the threshold. However our method more is adaptive than Tseng's and is capable to cope with various sinkhole attack.

6. Conclusion

In this paper, a sinkhole detection method based on incremental learning algorithm is proposed. As ad hoc networks has a changeable network topology, it is important for detecting model to catch up with recent network trends. The proposed method can adapt to the changes within a MANET and can find the sinkhole attack precisely. By experiment, we confirm that proposed method is well used not only for high typical sinkhole attack(high sequence number) but also for special version of sinkhole attack (stealthier attack) and robust to network environment

The future works will be to decide a, M, N value elaborately to reflect the network topology to lower the false positive rate and be a try to complement the method reducing computational complexity with the same sinkhole detection performance.

Reference

[1] Ad hoc network specific attacks held by Adam Burg

[2] 김신효, 강유성, 정병호, 정교일, “U-센서 네트워크 보안 기술 동향”, 전자통신동향분석, 제 20권, 제1호, pp. 93-99, 2005.

[3] H. C. Tseng, B. J. Culpepper, “Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators”,

[4] Lee kang hyen, “Detecting Inner Attackers and Colluded nodes in Wireless Sensor Networks Using Hop-depth algorithm”, IEEK journal vol 44-1, pp.113-121, 2007.

[5] Satoshi Kurosawa, et al "A Self-adaptive Intrusion Detection Method for AODV-based Mobile Ad Hoc Networks" Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on

[6] H. Ebbinghaus, Memory : A contribution to experimental psychology, Teachers College Press,1913.

[7] Y. an Huang, and W. Lee, “Attack Analysis and Detection for Ad Hoc Routing Protocols,” the 7th International Symposium on Recent Advances in Intrusion Detection (RAID’04), pp. 125 - 145,French Riviera, Sept. 2004.