A Detecting and Defending Method of Wormhole Attack Based on Time Ruler

Guoyuan Lv, Yiming Wang*, Canyan Zhu, Rong Chen, Lujie Wang
School of Electronics & Information Engineering
Soochow University,
Suzhou 215006, P.R.China
ymwang@suda.edu.cn*

***Abstract*—Wormhole attack is a severe attack in mobile ad hoc networks, which is particularly challenging to defend against. In this paper, a new method defined as time ruler using distance measurement for detecting wormhole attack is proposed including its hypothetical model, the concept of time ruler and the process of its establishment, storage and calibration. The feasibility of the method on theory, thus respectively deriving two discriminating inequalities with the use of sending time ruler and receiving time ruler are analyzed in detail. The performances of the method are also analyzed and its validity is evaluated with Omnet++ developing tools.**

Keywords-Ad Hoc networks; wormhole attack; attack detection; Time Ruler

I. INTRODUCTION

Mobile Ad Hoc networks (MANETs) are self-organized, multi-hop wireless networks which are independent of fixed infrastructure, with the advantages of easy networking and not being limited with time and space. Unlike the conventional network, MANETs are characterized by numerous constraints such as lack of infrastructure, lack of resources on nodes, dynamic topology, no centralized management and control, and lack of pre-established trust relationships between nodes. Due to these, MANETs are very likely to often be run in untrusted environments and make themselves vulnerable to various security attacks, such as eavesdropping, tamper, replay, and denial-of-service.

Wormhole attack is also called Tunnel attack. In MANETs, a malicious node records a packet, at one location in the network, tunnels the packet to another location, and replays it there. If the tunneled distance is longer than the normal wireless transmission range of a single hop, it takes less time or less hops to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route. In this case, it creates the illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors. Since it costs less hops to travel through tunnel than by a normal route, for shortest path routing protocol, the malicious node increases its attraction to network flow, and thereby providing advantageous conditions for itself to launch further attack such as tamper or packet-loss.

As to most routing protocols for Ad Hoc networks that exist such as AODV, DSR, DSDV, none of them are capable of defending against wormhole attack. There already exist some detecting and defending methods of wormhole attack, such as: Packet Leash, employing specialized hardware devices such as GPS [1], directional antennas [2], connectivity information approach based on visual network topology [3], and inserting new protocol to the nodes such as adding EnergyWatcher and TrustManager on the node [4]. These methods require accurate and fast calculation of nodes or high hardware equipment cost. And there were still many discussions on secure routing protocols against wormhole attack in the literatures recently [5], [6].

In fact, compared to normal single-hop link, the time that the pretended one through tunnel needs is much longer. Therefore, if normal nodes in the network can detect their single-hop distance from their neighbors, then they can detect this kind of tunneled links pretended to be single-hop, thus rejecting such malicious nodes around. The existing methods based on timing analysis can be divided into synchronous and asynchronous methods. The synchronous method requires the nodes to have tightly synchronized clocks but the drawbacks of the asynchronous methods is that they need to verify the vicinity of each neighbor by exchange instant and cooperated information from neighbors [7]. In this paper, we propose a new asynchronous method that does not have the drawbacks of the previous methods.

The remainder of this paper is organized as follows. Section II introduces a detecting method of wormhole attack based on time ruler with its hypothetical model. Section III analyses in detail the feasibility of the method on theory. Section IV offers the network performance results related to wormhole attack level in the circumstances that the method of timer ruler is applied to the networks suffering wormhole attack, and then verifies the effectiveness of this method. Finally, conclusion is given.

II. TIME RULER AND ITS ESTABLISHMENT, STORAGE AND CALIBRATION

For the convenience to define time ruler, we make the following assumptions:

(1) Every wireless transceiver of normal node i is provided with the same transmission radius $R(i) = R$.

(2) The network at least includes two malicious nodes, which are tunneled through wireless high-bandwidth channel out of band .We assume that malicious nodes won't join in the whole Ad Hoc network until all the other nodes have accomplished the job of initialization.

(3) Modified SAODV is applied to all the nodes. In addition to the original encryption of routing packets, we also encrypt the message of HELLO. Besides, some fields are inserted into HELLO for the use of setting time.

(4) The first routing packet sent is HELLO packet with affiliated information that is called HELLO_INFO. Any node is required to reply HELLO packet as an acknowledgement when it receives HELLO_INFO. Apart from the functions defined in AODV, HELLO_INFO and HELLO_ACK are mainly set for the established of time ruler.

(5) Each node has its own timing system .Time provided in different systems may not be exactly the same.

Every node sends routing packets in accordance with a certain rule. To be specific, they often send at the calculable time point with predetermined minimum intervals between two successive transmissions. The proposed concept of time ruler contains three elements: starting time to send routing packet T_0 , minimum interval between two successive transmissions G_t , allowed transmission range in one hop ΔT ($\Delta T = R/c$, c is the transmitted velocity of wireless signals in the free space). It is written as $Ruler:(T_0, G_t, \Delta T)$.Time points are marked from starting time with interval G_t infinitely.

In practice, each normal node is equipped with a sending time ruler $Ruler_{send,i}:(T_0, G_t, \Delta T)$ (i is the number of sending nodes) which is used for sending routing packets, and several receiving time rulers $Ruler_{receive,i\_j}:(T_0, G_t, \Delta T)$ (j is the number of some neighboring nodes) for the examination of receiving time corresponding to every adjacent node.

Every node should establish sending time ruler at the time of getting into network, with the process as follows:

Assumed that node S records sending time T_0 when it sends the first HELLO_INFO message, then calculates an allowed range ΔT based on its transmitted radius and sets an interval $G_t(S)$. Both of ΔT and $G_t(S)$ are sent appended to messages. Consequently, the sending time ruler of node S $Ruler_{send,S}:(T_0, G_t, \Delta T)$ is set up. Since then, node S has to send routing packets exactly according to calibrations $T_k = T_0 + kG_t(\mathrm{S})\ (k = 1, 2\mathrm{L})$ marked on the sending ruler. A node can't change its sending ruler once established until it exits from this network.

The neighboring node (A as supposed) will reply with HELLO_ACK after receiving the message of HELLO_INFO from S. The period of time when HELLO_ACK transmits from A to S is written as t_d .Later node S records arriving time T_r as it receives HELLO_INFO from A. Then the beginning point of sending time can be calculated as $T_0 = T_r - t_d$. On the other side, allowed range $\Delta T = R(A)/c$ and interval $G_t(A)$ taken from A's HELLO_INFO are regarded as ΔT and G_t of receiving time ruler. In that case, the receiving time ruler $Ruler_{receive,S\_A}:(T_0, G_t, \Delta T)$ of node S corresponding to node A eventually sets up.

As a normal node, node i has only one sending time ruler, but several receiving rulers when several neighbors are around it. All the scales on the time ruler can be easily acquired through calculation as long as the three elements are certain. Owing to that, we only need to store them three. Hope that links to all the adjacent nodes can be detected separately, node i stores receiving time rulers in accordance with neighboring nodes list, so that it is easy to figure out receiving time ruler referring to identity information from its neighbors(such as IP or MAC address). Because of the transmission time between the sending note and neighbors, the beginning point of sending time needs calibration. Furthermore, neighbor validity states need update. Thus, the neighbor list of a note includes IP/MAC address, receiving time ruler $Ruler_{receive,i\_j}:(T_0, G_t, \Delta T)$, calibration flag (CF) and neighbor validity states (NVS).

III. BASIC PRINCIPLE FOR DETECTING WORMHOLE ATTACK WITH TIME RULER

After all the neighboring nodes of Ad Hoc network have linked together, they must send routing packets following its already designed time ruler. Each receiving node decides whether the route of packet is valid or not according to receiving time ruler of the sender (learned from routing packets).The receiving moment of routing packet ought to be predictable if the distance between the sender and the receiver is variable but not further than the transmission radius since packets are transmitted with specific intervals. Generally, the effective neighbors and wormhole attack can be detected by the sending time ruler or receiving time ruler.

A. *Finding effective neighbors with sending time ruler*

Nodes in the Ad Hoc can enter or leave at any time. The node will first broadcast one-hop message of HELLO to establish its direct links with others when it joins in the Ad Hoc network. All the routing messages including HELLO are required to send in accordance with sending time ruler.

In Fig.1, node S detects valid neighbors by the means of checking other nodes with replied HELLO_ACK. In the coverage range of node S exists normal node A and malicious node M1 while the normal node X covers normal node B and malicious node M2. The gap between M1and M2 that is longer than any radius of all the nodes is tunneled by wireless high-bandwidth channel out of band.

Assumed that the distance between S and X is longer than the transmission radius $R(S)$ of node S, and also exclude the delay of the routing messages on the node, the HELLO_ACK message sent by node X and node A will reach at different time.

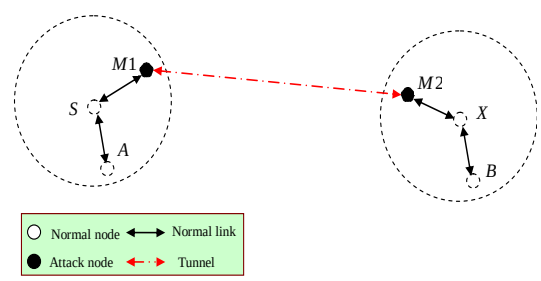

Figure 1. Wormhole detection principle

The sending time ruler $Ruler_{send,S}:(T_0,G_t,\Delta T)$ is established as node S sends a message of HELLO_INFO. This message reaches node X through the tunnel between M1 and M2 after it arrives at node A by normal channels. However it can't get to node B due to its short life span of only one hop. Node A and X will answer with HELLO_ACK immediately or after several delays of G_t, so the time points that node A and X receive HELLO_INFO can be obtained as follows:

$$t_{Ar}=T_0(S)+d(S,A)/c+\Delta t_{sys}(A,S) \quad (1)$$

$$t_{Xr}=T_0(S)+\left(d(S,M1)+d(M1,M2)+d(M2,X)\right)/c+\Delta t_{sys}(X,S) \quad (2)$$

Supposed that node S is within the coverage of node A and M1, then the time points of node S that receives HELLO_ACK from node A and node X are

$$t_{SAr}=t_{Ar}+k_1G_t(S)+d(A,S)/c+\Delta t_{sys}(S,A) \quad (k_1=1,2...) \quad (3)$$

$$t_{SXr}=t_{Xr}+k_2G_t(S)+\left(d(X,M2)+d(M2,M1)+d(M1,S)\right)/c+\Delta t_{sys}(S,X) \quad (k_2=1,2\cdots) \quad (4)$$

respectively.

Where, $\Delta t_{sys}(S,A)$ and $\Delta t_{sys}(S,X)$ represent deviations of system time between node S and A, node S and X, besides: $\begin{cases}\Delta t_{sys}(S,A)=-\Delta t_{sys}(A,S)\\ \Delta t_{sys}(S,X)=-\Delta t_{sys}(X,S)\end{cases}$

Put (1)(2) into(3)(4)separately, as long as return time t_{SAr} meets the condition :

$$T_0(S)+kG_t(S)<t_{SAr}<T_0(S)+kG_t(S)+2\Delta T \quad (k=1,2L) \quad (5)$$

whether A is the effective neighbor of node S can be figured out.

Generally speaking, When these nodes send messages is unknown, the deviations of arrival time are usually obtained by taking the remainder of G_t .The time difference from sending HELLO_INFO to receiving HELLO_ACK by node S to A and X are $\Delta t_{Ad}=t_{SAr}-T_0(S)$ and $\Delta t_{Xd}=t_{SXr}-T_0(S)$, respectively.

Considering $d(A,S)=d(S,A)$, we can get:

$$\Delta t_{Ad} \bmod G_t(S)=2d(S,A)/c<2R/c=2\Delta T \quad (6)$$

$$\Delta t_{Xd} \bmod G_t(S)=2\left(d(S,M1)+d(M1,M2)+d(M2,X)\right)/c>2R/c=2\Delta T \quad (7)$$

Illustrated as Fig.2, due to the existence of tunnel, the remainder of the time deviation back from node X is larger than $2\Delta T$, however that of normal node is less than $2\Delta T$. Hence, node A is judged as an effective neighbor of node S, but node X is not.

B. Detecting tunnels and update the list of neighbor nodes using receiving time ruler

Owing to the mobility of wireless network, the active state of notes is not always constant. Though the node can recognize neighbors' validities by the means of periodically broadcasting HELLO affiliated with sending time ruler, frequent broadcasting and replying will increase the cost of network. Here a method using receiving time ruler to continue checking neighbors in the list for their validity is proposed.

In Fig.1, S is assumed as a new entrant or a node just moving in, node A and node X rebroadcast HELLO_INFO based on their former sending ruler, so that node S can establish its receiving time ruler corresponding to node A or node X.

Node S calculates and stores the receiving time ruler related to sender A $Ruler_{receive,S\_A}:(T_0,G_t,\Delta T)$ when it receives HELLO_INFO from A.

Later, node A sends routing packet at a time point on its sending time ruler, reaching node S at the time $t=t_{Sr}$.

$$t_{Sr}=T_0(A)+mG_t(A)+d(A,S)/c+\Delta t_{sys}(S,A) \quad (m=1,2L) \quad (8)$$

Then node S checks whether receiving time t_{Sr} is within the scope of sender's receiving time ruler that corresponds to sender.

When $d(A,S)$ ranges from 0~ R_A , then arriving time matches:

$$T_0(A)+mG_t(A)<t_{Sr}<T_0(A)+mG_t(A)+\Delta T \quad (m=1,2...) \quad (9)$$

The inequality will be:

$$0<\Delta t_{Ar} \bmod G_t(A)<\Delta T \quad (10)$$

Node S will set node A as invalid state in its neighbor list, if it does not matches with (10), otherwise valid. In a similar way, node S establishes receiving time ruler corresponding to node X. Accordingly, it can figure out whether node X is valid neighbor or not.

Furthermore, when node A moves out of the coverage range of node S which is similar to the S with X condition in Fig.1.When node S receives routing packets from node A, it will set node A invalid in the neighbor list. Fig.3 directly reveals the difference of receiving time when the distance between S and A is in the transmission range or not.

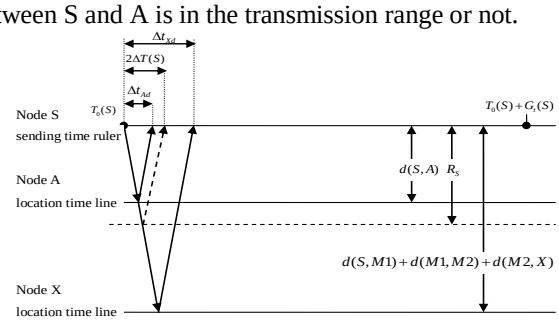

Figure 2. Neighbor validity detection with sending time ruler

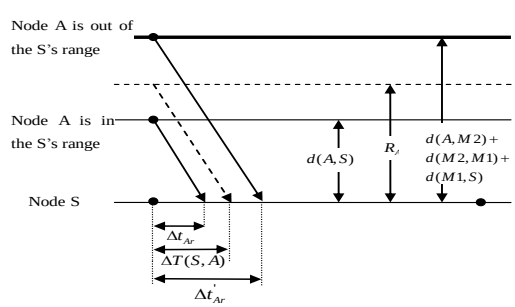

Figure 3. Neighbor validity detection with receiving time ruler

IV. SIMULATION AND EVALUATION

We use Omnet++4.1 network simulator to simulate and implement this detecting method of wormhole attack based on time ruler. In the simulated network, 50 nodes, including 5 source nodes and 5 malicious nodes, are distributed randomly in a 2000×2000 m^2 two-dimensional ground. The transmission range of all normal nodes is a circular area with the radius of 323 m, while the maximum length of tunnel between malicious nodes could be more than 1000 m. All nodes move with the speed of 1～10m/s in a random but limited-moving model, which means that they first choose a direction in the range of 360 degrees before moving, then move a fixed distance in a constant velocity. After reaching the destination, they rest for a while and change to another random direction, and again move a fixed distance in a certain speed. The routing protocol of SAODV is applied to all the normal nodes, and wormhole malicious nodes use the same model as normal nodes. The tunnel will be built if the distance between malicious nodes is greater than their transmission range R, but shorter than the tunnel's maximum length, otherwise, the tunnel building fails. Malicious node won't send data or routing messages on its own initiative, but instead just forward routing messages from other nodes and discard data messages. Normal nodes will isolate them as soon as they detect attack ones. In this way, the detection of malicious nodes can help reduce loss rate of data packets.

Fig.4 shows the relationship between loss rate of network packets and node mobility before and after using the method of time ruler detection. When this method is not applied (curve I), the loss rate is about 35%, and40% at most, while afterwards, it reduces a lot. While the loss rate is around 12.5～25% if the time ruler has an interval G_t 6 times of ΔT (curve II), it will decrease to 11～20% when the interval adds to 12 times of ΔT (curve III).What's more, in the case of the same node mobility, the latter's loss rate is always a little smaller, which indicates that the time ruler whose interval is longer will have lower loss rate, and obviously better performance of the entire network.

In addition, two phenomena shown after application of this method need further explanation.

First, when nodes have constant speed, the time ruler with longer intervals results in better network performance, which is consistent with analysis above. Precisely, as to normal nodes with fixed transmission range, its probability to detect illegal link is related to the interval G_t .When the time ruler applied in the network suffering wormhole attack possessed a larger value of G_t ,the probability to discover wormhole will increase, thus more wormholes will be detected and isolated by normal nodes.

Second, concerning a time ruler with constant interval G_t , the network performance improves in the wake of increase in the speed of nodes. As a whole, in a certain period, when nodes speed up, every normal node can get direct contact with more other nodes, therefore establishing more receiving time rulers. When the number of receiving time ruler established boosts, the probability to discover wormhole will

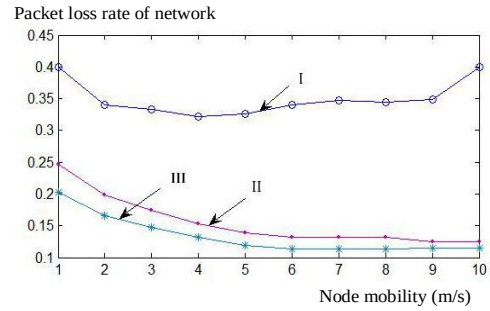

Figure 4. Wormhole simulation

increase, thus more wormholes will be detected and isolated by normal nodes.

V. CONCLUSION

In Ad Hoc network, wormhole attack is more difficult to defend against. As to wormhole attack building tunnels on the channel out of band, it is characterized by its length that is much longer than single-hop of normal nodes. Therefore, the tunnel can be detected as long as the length of the single-hop link is obtained. Since the propagation speed of messages between nodes is determined, measuring the propagation time of the message can reach the purpose of measuring length of the link.

ACKNOWLEDGMENT

The work is supported by National Natural Science Foundation of China under Grant No. 61172056, Doctoral Foundation of Ministry of Education of China under Grant No. 20093201110005.

REFERENCES

[1] W. Wang, B. Bhargava, Y. Lu and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks," Wireless Communications and Mobile Computing, vol. 6, June 2006, pp. 483–503.

[2] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," Network and Distributed System Security Symposium, San Diego,CA,5-6 February 2004.

[3] Dezun Dong, MoLi, Yunhao Liu, Xiang-Yang Li,and Xiangke Liao, "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks,",IEEE/ACM Trans. Networking, vol. 19, no.6, December 2011, pp.1787-1796.

[4] Guoxing Zhan, Weisong Shi, and Julia Deng, " Design and Implementation of TARF:A Trust-Aware Routing Framework for WSNs," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, March/April 2012, pp.184-197.

[5] Michele Nogueira, Helber Silva, Aldri Santos, and Guy Pujolle, "A Security Management Architecture for Supporting Routing Services on WANETs," IEEE Trans. Network & Service Management, vol. 9, no. 2, June 2012, pp. 156-168.

[6] Juan A. Martinez, Daniel Vigueras, Francisco J. Ros, and Pedro M. Ruiz,"Evaluation of the Use of Guard Nodes for Securing the Routing in VANETs," Journal of Communications & Networks, vol. 15, no. 2, April 2013, pp.122-131.

[7] Majid Khabbazian, Hugues Mercier, and Vijay K. Bhargava, " Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks," IEEE Trans. Wireless Communications, vol. 8, no. 2, February 2009, pp.736-745.