International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.181-192
http://dx.doi.org/10.14257/ijsia.2016.10.5.17

Research on Wormhole Attack Detection Algorithm in Space Information Networks

Yu Geng[1] ,Zhang jie[2] ,Zhang Yongfang[2],Ye ning[2] and Ren Kaiya[3]

[1.] *Shenyang Aerospace University, Shenyang Liaoning china*
[2]. *Northeastern University, College of information science and Engineering, Shenyang Liaoning china*
[3.] *Air force of Chengdu Military Area Command china*
yug@sau.edu.cn;772863496@qq.com

Abstract

Wormhole attack is a coordinated attack that launched by two or more malicious node. With a high quality private link malicious node, attracted traffic, attacked routing protocol, destroyed network topology, has a great threat to space information network. We propose a wormhole attack detection algorithm based on abnormal topology and time delay in space information network and the algorithm is mainly composed of two phases: finding abnormal topology and getting the malicious node. According to the number of nodes which are mutually non-one-hop neighbors in the normal network and the abnormal topology in backbone get the suspicious neighbors. To confirm the fake link, uses the round trip time to detect suspicious neighbors. Sends warning messages to isolate false neighbors or malicious nodes to ensure the security of the network. Using the network simulation software NS2 analyses the performance of the detection algorithm. The simulation results show that the proposed algorithm can detect wormhole also has high detection rate and a low false positive rate.

Keywords*: Space information network; wormhole attack; time delay; abnormal topology*

1. Introduction

The space information network is composed of satellites, common flight vehicles and ground nodes which have the ability to communicate with each other. The nodes are heterogeneous and exposed to the space. The information is easy to obtain and suffer from a wide variety of attacks. Especially suffer in wormhole attack which is a coordinated attack that launched by two or more malicious node. Firstly, to build a private link, which is a high bandwidth and high quality link, can be called "tunnel". In order to launch attack, the distance of the tunnel is far greater than the normal transmission distance. The message gets through the "tunnel", and then re-injected into the network. Wormhole attacks can bypass the encryption, authentication, direct damage of the network topology, thus formatting a variety of network attacks. Currently, Efficiency defensive measures in space information network are not related to the wormhole attack. Therefore, it is very important to study the wormhole attack detection algorithm for space information network.

In recent years, researchers have been studying on the wireless network, according to the characteristic behavior of wormhole attacks, some defensive algorithms have been proposed to detect wormhole attacks. Literature [1-3] for the transmission distance of "wormhole tunnel" is much larger than normal nodes. So the two pseudo neighbor nodes delay is longer than the two normal neighbor nodes. The round-trip delay (Round Trip Time, RTT) or packet time limit are used to detect and prevent wormhole attacks. These

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2016 SERSC

mechanisms do not require additional hardware, but the detection effect is not good, the wormhole attack will seriously damage the normal network topology.

Literature [4-5] proposed an algorithm for finding prohibited network structure to detect wormhole attacks, using the link information in the connection diagram to find the forbidden substructures. This algorithm does not require special hardware equipment and location information, which is suitable for the large node density network, but with some limitations. The algorithm was used to identify the nodes in the network by the Sookhak Adnan and Akhundzada Mehdi [6], with the help of credit mechanism and location; In addition it depends on node location and key mechanism in the network.

The algorithm requires a number of key exchanges. There are also some hybrid detection algorithms, such as: [7-8] *et al* proposed the combination of wormhole delay mechanism and topology mechanism, this mechanism requires a network with certain restrictions, such as isomorphic nodes and time synchronization *etc*., which with high implementation complexity.

In view of the above research question, according to the behavior characteristics of the wormhole attack, it's different to detect wormhole attacks in MANET. In this paper, according to the space information network the network nodes are divided into different levels and links, so space information network is divided into ordinary nodes network and satellite backbone network. According to the common node network topology of wormhole anomaly characteristics and satellite backbone network node link formation features that are required to meet the conditions, satellite link of wormhole nodes anomaly detection is proposed. In the end, the topology anomaly information is combined with the delay, which is confirmed by the time delay detection mechanism, which is used to isolate the network and ensure the security of the space information network.

The rest of this paper is organized as follows. In the second part, the paper introduces the implementation of the algorithm in detail. The third part is the simulation of the proposed algorithm WADA. The fourth part will be summarized in this paper.

2. Detection Algorithm in Space Information Network

2.1. Abnormal Topology Searches

(1) Search on ordinary node abnormal topology

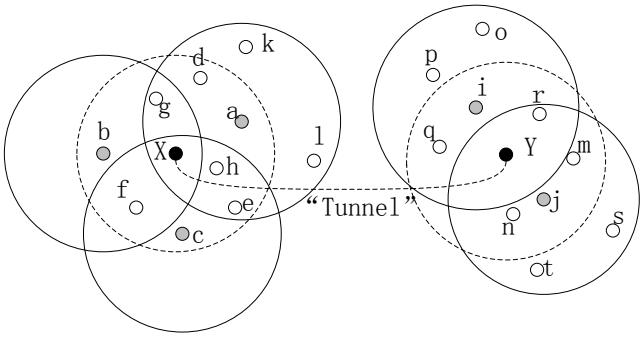

Figure 1. The Network Topology of Wormhole Attack

Yun Wang *et al*. [9] presented that the normal network had normal topology. In normal networks, the two-hop neighbors had only up to two common one hop neighbors. In addition, the two one hop neighbors usually had the same hop neighbors. When suffer in wormhole attack, between the two pseudo neighbors do not have a neighbor with one real jump. As shown in Figure1, wormhole attack is formed between node X, and Y, one hop neighbor node a: $N_1(a) = S_1(a) \bigcup T_1(a) = \{i, j, m, n, r, q\} \bigcup \{d, k, e, l, g, h\}$, one hop

 Copyright ⓒ 2016 SERSC

neighbor node i: $N_1(i) = S_1(i) \bigcup T_1(i) = \{a,b,c,d,e,f,g\} \bigcup \{o,p,q,r\}$, $T(a) \bigcap T(i) = \varnothing$ There is no same true neighbors between them, but $S_1(a) \bigcap T_1(i) = \{q,r\} \neq \varnothing$ 。 According to the above-mentioned two topological properties can detect whether the network is attacked by the wormhole attack.

(2) The search for the abnormal topology of satellite backbone network

The behavior characteristics of the satellite nodes make the network topology have a certain periodicity and predictability. According to the known topological structure and the establishment of inter satellite links, we can judge the abnormal structure of satellite networks.

1. The division of time slices to create a virtual topology snapshot

Time slice is divided into two classes: the inter rail link and the inter layer link time slice. And the common Walker constellation [10] is used to give the Walker constellation.

As shown in Figure 2, the inter satellite link is established to meet the requirements of establishing the inter layer link between LEO and MEO satellites. The need to meet the LEO satellite in the coverage of the MEO satellite and the communication angle between them is greater than the minimum angle. When communication angle is greater than the minimum communication angle $\varepsilon_{\min}$, ψ denotes the angle between the satellite M of MEO in the coverage of LEO. And the formula is shown in the formula:

$$\psi = \frac{\pi}{2} - \varepsilon_{\min} - \arcsin(\frac{R_L}{R_M}\cos\varepsilon_{\min}) \quad (1)$$

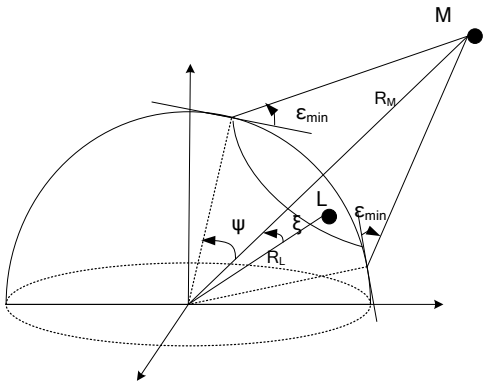

Figure 2. The Establishment of the Link between the Layers

When a communication link is established, it should be satisfied $\xi < \psi$, as shown in formula:

$$\xi = \arccos(\frac{R_M^2 + R_L^2 - \left|\overrightarrow{LM}\right|^2}{2R_M R_L}) \leq \psi \quad (2)$$

$\left|LM\right|$ can be denoted by the two nodes. In any time, Walker constellation in the coordinates of a satellite can be expressed by formula (3).

$$\begin{cases} x = R\cos k\sin j\sin\alpha + R\sin k\cos j \\ y = R\cos k\sin j\sin\alpha + R\sin k\cos j \\ z = R\cos k\sin\alpha \end{cases} \quad (3)$$

α denotes the satellite orbital inclination. j denotes the angle between the satellite orbital plane and the intersecting line of xoy and y-axis positive axle. $k = \omega t + k_0$ denotes the temporal phase satellites of t. Using formula (1), (2), (3) to calculate the time of LEO and MEO is established and off, the calculation result is a series of time values, time alternation said that the link establishment and disconnection between the two satellites. So does the MEO satellite layer. At the beginner, assuming t=0 and this time point set $\Gamma_{L_{1,1}}^{M}$ is empty. MEO satellite layer comparison between the current time and the presence of link layer, select the max link off time of MEO to denote satellite M as the access satellite. Assuming t_1 denotes the time of the link off, thus $L_{1,1}$ of $[t_0, t_1]$ can only establish communication link with M. t_1 denotes one point of the set $\Gamma_{L_{1,1}}^{M}$. Assuming t_1 is equal to t, repeat the above process to obtain a link exists an inter-layer between MEO and $L_{1,1}$ at any time. Similarly, you can get Γ_{M}^{G} and the inter layer-link between MEO and GEO. Γ_{L}^{G} and layer-link between LEO and GEO.

Through the research on the rail link and the layer link between on-off state can get the time set, then to seek union and get the time set of the satellite network in one operation cycle time, which established the link relationship between satellite network topology structure and each satellite at any time.

3 inter satellite link

In satellite communication, two conditions are met, the communication between the two satellites is greater than the minimum communication angle and the two satellites are in the same range of the antenna.

As shown in Figure 3, $(x_i,y_i,z_i)$and(x_j,y_j,z_j) denote the coordinate of the satellites i and respectively ε denotes the communication angle between i and j.Assuming the satellite i has the minimum communication angle $\varepsilon_{\min}$, the satellites i and j can establish the communication link between them only if $\varepsilon < \varepsilon_{\min}$.

$$\sin\varepsilon = \cos\lambda = \frac{\vec{oj} \bullet \vec{ji}}{\left|\vec{oj}\right|\left|\vec{ji}\right|} = \frac{x_j(x_i - x_i) + y_j(y_i - y_j) + z_j(z_i - z_j)}{\sqrt{x_j^2 + y_j^2 + z_j^2}\sqrt{(x_i - x_i)^2 + (y_i - y_j)^2 + (z_i - z_j)^2}} \geq \sin\varepsilon_{\min} \quad (4)$$

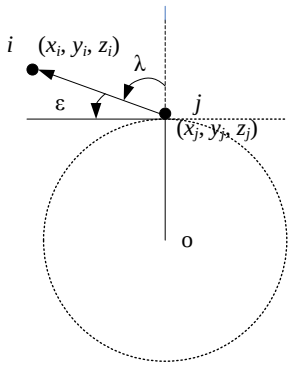

Figure 3. Schematic Diagram of Elevation

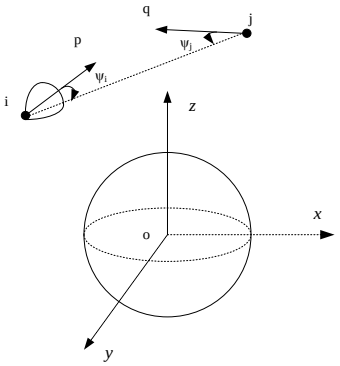

Figure 4. Schematic Diagram of Antenna

 Copyright ⓒ 2016 SERSC

International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.181-192
http://dx.doi.org/10.14257/ijsia.2016.10.5.17

In Figure 4, i and j denote communication satellites, they are known in the coordinate system, $2\alpha_i$ and jq denote the antenna orientation of satellite i and j, and $2\alpha_i$ denotes the beam width. ψ_i and ψ_j denote the angle between jq and ij .If the satellites i and j can establish the communication link , only if the antenna beam of satellite j should be in the range of the satellite i and $\psi_j < \alpha_j$. ψ_i can be denoted by i, j and p. So does ψ_j .

In the satellite backbone network, we first judge whether the satellite node i is a suspicious neighbor, and check if the neighbor is in the static neighbor table, if not, and use of formula (4) and (5) to determine the establishment of the link. Node i send a cooperative detection packet to the node j, and then repeat the process of Step2. After the cooperative detection and the link between i and j is detected, put the result to the node i, namely the link structure is abnormal.

$$\psi_i = \arccos \frac{(x_p - x_i)(x_j - x_i) + (y_p - y_i)(y_j - y_i) + (z_p - z_i)(z_j - z_i)}{\sqrt{(x_p - x_i)^2 + (y_p - y_i)^2 + (z_p - z_i)^2}\sqrt{(x_j - x_i)^2 + (y_j - y_i)^2 + (z_j - z_i)^2}} \quad (5)$$

2.2. Confirm the Malicious Node of Wormhole Attack

1. The theory of detection

Each node records its own forwarding time of RREQ and RREP time, and calculates the time, that is denoted by RTT to the destination node. In Figure 5, the RTT from intermediate node A to the destination node D can be expressed as $RTT_{A,D} = TA_{REP} - TA_{REQ}$ .The RTT from intermediate node B to the destination node D can be expressed as $RTT_{B,D} = TB_{REP} - TB_{REQ}$,The intermediate node will put the real results into the RREP and send to the source node.

The source node is responsible for collecting all the RTT values and calculating the RTT values between each hop node. Because of the existence of the wormhole "tunnel", the round-trip time-delay of the suspicious neighbor tends to be larger than the normal. Therefore, take advantage of the abnormal of round trip delays to confirm which suspicious neighbors, to find abnormal delay link are. The nodes will be suspected When the RTT values of the two nodes satisfy the formula $RTT \geq 2 \times RTT_{\max}$.

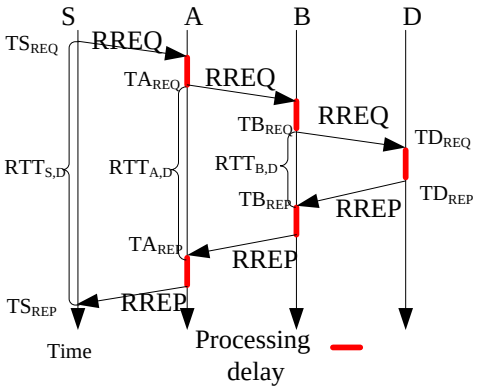

Figure 5. Time of Forwarding RREQ and Receiving RREP

Different from satellite nodes, the communication radius of the common nodes is equal, so the maximum value RTT of each node is the same. The formula for calculating the maximum value of $RTT_{\max} = 2R/V$ 。(R denotes the maximum transmission radius for the node, V denotes the transmission rate of light)

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2016 SERSC

Taking into account the change of the node position in the satellite backbone network, the average value of the sending and receiving packets is used as the final time delay. When data packets are sent, getting the coordinates of the two satellites (x_i, y_i, z_i) and (x_j, y_j, z_j), the link delay $t_{i\to j}$ is calculated by using the velocity distance formula. At the end of the data packet, the coordinates of the two satellites are $\left(x_i^{'}, y_i^{'}, z_i^{'}\right)$ and, $\left(x_j^{'}, y_j^{'}, z_j^{'}\right)$ and the link delay $t_{i\to j}$' between the two satellites is calculated. The RTT value is the sum of the two.

2. The process of detecting

Step 1: the source node broadcasts a HELLO message, and the time of the local record is recorded. The number of hops limit is set to 2, which limits the scope of the HELLO broadcast.

Step 2: after the node receives the HELLO message to add their own information, and then in accordance with the original path to reply to a ACK message. And the number of hops minus 1, if subtract 1 is not equal to 0, and rebroadcast the modified HELLO message, also record the time of the broadcast HELLO message.

Step 3: the node receiving the ACK message will record the time of the ACK message, and then calculated RTT with the ACK sender according to the formula $RTT = t_r - t_s$. The result of RTT is appended to the ACK message and forwarded to the next hop node. If the destination node's ID the same with its own ID, judging ACK message comes from one-hop neighbor or two-hop neighbor. They are neighbors if there is only one node in the path field, and get the value of RTT. If the path field has two nodes, they are the 2-hop neighborhood, and check the RTT which is added to the ACK message.

Step 4: the use of formula (6) to determine whether the one hop neighbor nodes and 2-hop neighborhood are suspicious. For a hop neighbor, if the RTT satisfies the formula (6), the neighbor node is a false neighbor, which records the list of false neighbors, else the node record in the trusted neighbor list. As for the two-hop neighbors, if the ACK message in the RTT satisfies the formula (6), it is represented as a two hop pseudo neighbor, and records it in the two hop false neighbor list, then record the path in the corresponding position. Otherwise, record it in the two hop trusted neighbor list. The isolation of pseudo neighbors, wormhole link will be excluded from the network.

 Copyright ⓒ 2016 SERSC

3. Performance Evaluations

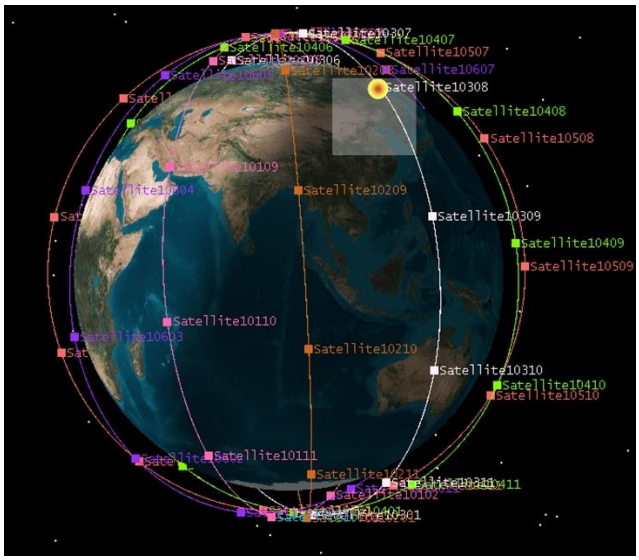

Figure 6. Simulation Scenario

The simulations were programmed in C using AODV routing protocol and node distribution models from NS-2. We considered the simulation scenario shows in Figure 6, the topology with N+66 nodes placed uniformly in fixed area. In order to facilitate the test detection algorithm, we simulated the iridium system, set up satellite node 66(The network topology is fixed, and the link can be judged.) also set random dynamic node N.

A: Network performance

We set up N=200 and have 10 malicious nodes and there are 30 pairs of communication nodes in the network. we test network packet delivery ratio in different sending rate. As shown in Figure 7, with increase of the contract rate, packet delivery rate decreases and the wormhole attacks on the network packet delivery ratio have a serious impact.

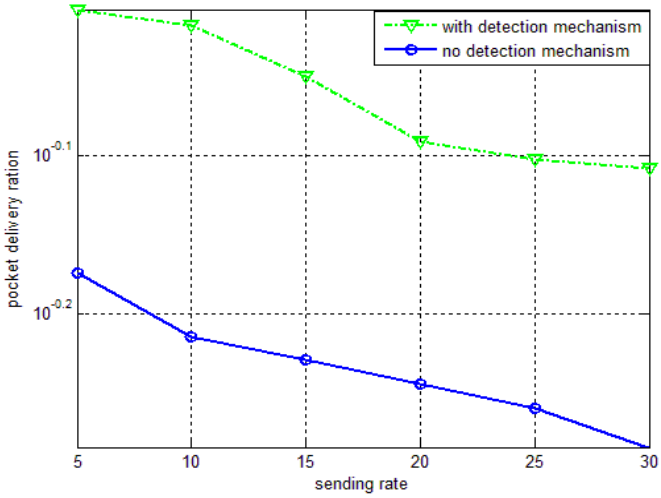

Figure 7. Packet Delivery Ratio vs. Sending Rate

To testing the effects of wormhole attack defense mechanism on the throughput of the network, Figure 8 shows the throughput changes under wormhole attack without safety. Wormhole attack causes the network cannot be in accordance with the optimal routing for routing and affects the network throughput.

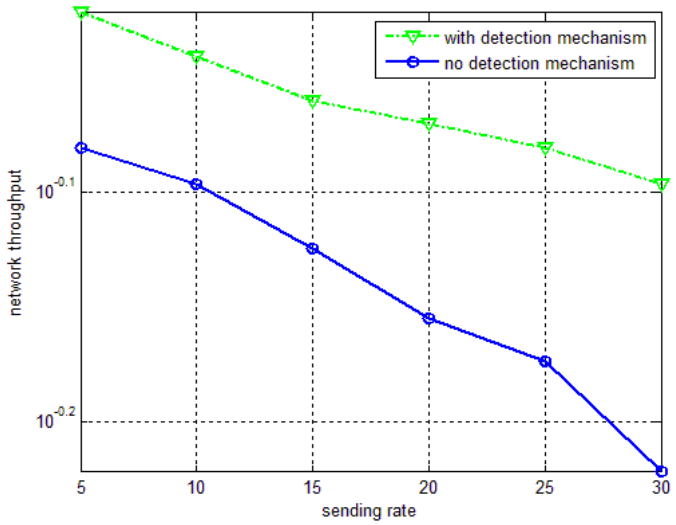

Figure 8. Network Throughput of Wormhole Attack

B: Comparison of the Algorithms

Use detection ratio of attack and the error of false neighbors for evaluating the performance of wormhole attack detection algorithm (WADA) and contrast with RTT algorithm [2], WDI algorithm [7], and TCBWD algorithm [11].

In order to verify the effect of wormhole attack detection algorithm in different length “tunnel” with {2,3,4,5,6} hops. Figure 9.reflects that the attack detection rate of the three detection algorithms gets higher with the increase of the length of tunnel. WADA algorithm combined with neighbors information detection, which has the highest probability of the detection under variety of "tunnel" length, the detection ratio of attack more than 0.9. In Figure10. shows the error rate of the "tunnel", which reflects the comparison between the two algorithms of RTT and WADA.

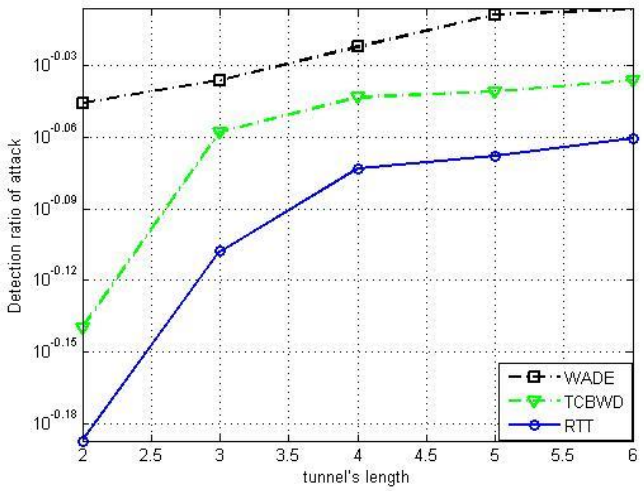

Figure 9. Detection Ratio of Attack vs. Tunnel’s Length

Copyright ⓒ 2016 SERSC

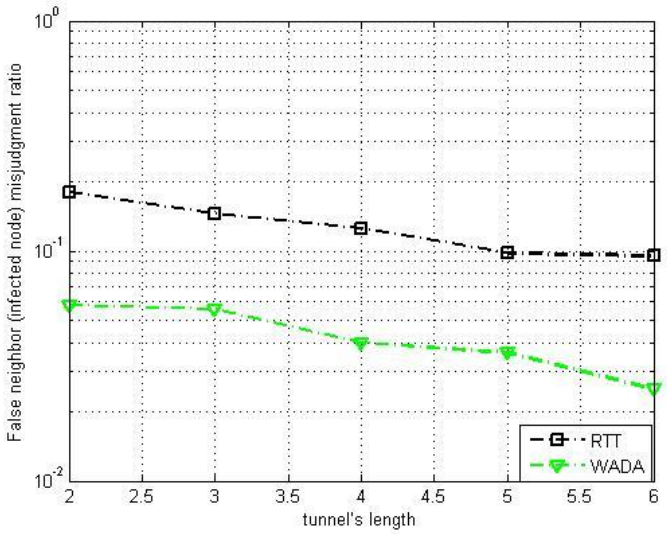

Figure 10. False Neighbor (Infected Node) Misjudgment Ratio vs. Tunnel's Length

Verify the influence of detection algorithm for detecting wormhole attacks in different network densities, N belongs to the set {50,100,150,200,250}; Figure 11 and Figure 12 are a comparison of the two detection algorithms of WDI and WADA. The attack detection rate of WADA in the same density is higher than WDI. Due to the increase in the density of nodes, the possibility of the nodes in the intersection are not attacked is increasing.

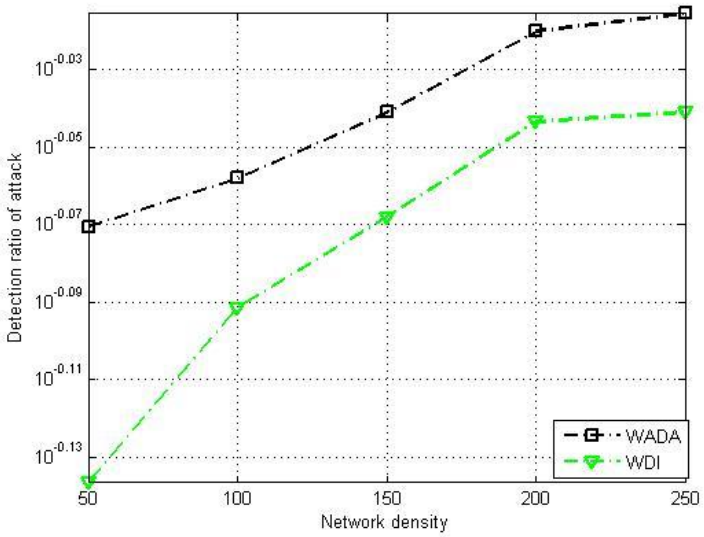

Figure 11. Detection Ratio of Attack vs. Network Density

4. Conclusions

In this paper, according to the wormhole attack of the space information network, we put forward a wormhole attack detection algorithm which is based on topological anomalies and delay in space information network. The detection algorithm is divided into two stages. It's including abnormal topology search and malicious nodes judgment

Copyright ⓒ 2016 SERSC

In the stage of searching abnormal topology, the suspicious nodes are judged by comparing the abnormal topology of normal nodes and the abnormal topology of satellite networks. Get one hop and two hops suspicious neighbors by using topological anomalies then more recent confirmation is determined by the delay characteristics. Finally, to protect the security of the network a warning message is sent to isolate a false neighbor node or a malicious node. Simulation analysis of the proposed algorithm is achieved through the use of NS-2 network simulation software and the results show that the algorithm can detect wormhole attacks, and has a higher detection rate and lower false rate of wormhole attack.

Acknowledgements

This reach was supported by National Natural Science Foundation of China under grant (U14331156, 61401079, 1151002, 61401079, 61501038) and by China Aerospace Science and Technology Corporation Satellite Application Research Institute Innovation Fund under grant 014-CXJJ-TX-11 and by Special Fundamental Research Fund for Central Universities under grant N120404003.

References

[1] S Shamaei, A Movaghar. A Two-Phase Wormhole Attack Detection Scheme in MANETs [J], the ISC Int'l Journal of Information Security, **(2014)**, 6: pp. 183-191.
[2] V K aju, Kumar K V. A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks In Mobile Ad Hoc Networks [A], 2012 International Conference on Computing Sciences [C], Phagwara, **(2012)**, pp. 271-275.
[3] A Saeed Alshamrani. Packet Travel Time Algorithm in Mobile Ad Hoc Networks [A], 25th IEEE International Conference on Advanced Information Networking and Applications Workshops [C], Los Alamitos, 2011, 561-568.
[4] R Maheshwari, J Gao, D S R. Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information [A], 26th IEEE International Conference on Computer Communications [C], Anchorage, **(2007**, pp. 107-115.
[5] C H, Lou W, Wang Z. Securing DV-Hop localization against wormhole attacks in wireless sensor networks[J]. Pervasive and Mobile Computing, ,vol. 16, **(2015)** pp. 22-35.
[6] M Sookhak, A Akhundzada. Geographic Wormhole Detection in Wireless Sensor Networks [J], DOI:10.1371/journal.pone.0115324 January 20, **(2015)**.
[7] H Mahriyar, M Ali Azimi Kashani. A New Method for Preventing Wormhole Attacks in Wireless Sensor Networks [J],Advances in Environmental Biology, vol. 8, no. 10, June **(2014)**, pp. 1339-1346 .
[8] M Sookhak, A Akhundzada, A Sookhak. Geographic Wormhole Detection in Wireless Sensor Networks [J]. PloS one, vol. 10, no. 1. **(2015)**.
[9] Y Wang, Z Zhang, J Wu. A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information [A], 2010 IEEE International Conference on Networking, Architecture and Storage [C], Macau, pp. 63-72, **(2010)**.
[10] C She, J Wang. Dynamic analysis of Walker constellation satellite network topology [J], Journal of communication, vol. 27, no. 8, **(2006)**, pp. 45-51.
[11] K. S. Chan and M. Alam, "Tcbwd: Topological comparison-based byzantine wormhole detection for Manet," in Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on, oct. **(2011)**, pp. 388 –394.

Authors

Yu Geng (1973-) Male, Shenyang Liaoning, PhD of Beijing University of Aeronautics and Astronautics, Professor of Shenyang Aerospace University. The main research direction is the aviation moving from the organization network, general aviation flight dynamic monitoring, *etc*. E-mail: yug@sau.edu.cn.

 Copyright ⓒ 2016 SERSC

Zhang Jie(1991-) Male, Chongqing Tongliang, Graduate students of Northeastern University. That mainly research on the security of spatial information network. E-mail: 772863496@qq.com

Copyright ⓒ 2016 SERSC

Copyright ⓒ 2016 SERSC