ISSN 2320-9984

Volume 6 Issue 2 | June 2018

ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Wormhole Attack Detection in Wireless Network Using Constraints-Based Function

Haritima Shrivastava
M.Tech. Research Scholar Software Engineering
Oriental Institute of Science and Technology
Bhopal, (M.P.) [INDIA]
Email: haritimashrivastava@gmail.com

Bhupendra Panchal
Head of the Department
Department Of Computer Science & Engineering
Oriental Institute of Science and Technology
Bhopal, (M.P.) [INDIA]
Email: bhupendrapanchal30@gmail.com

Abstract—*Security and access control of data is major issue in wireless network. The mobility and open stack of communication of wireless networks intended various security threats. In wireless network some well know attacks such as black hole attack, wormhole attack degrades the performance of network and theft of data. in this paper proposed the constraints-based function for the detection of wormhole attack. The constraints-based function used clustering and round-trip time (RTT). The process of algorithm estimates the position of worm node using the value of distance function K. the proposed algorithm simulated in NS-2 simulator and evaluate some standard parameters. Our proposed algorithms give better performance instead of pervious algorithm of wormhole detection.*

Keywords:— *Wireless Network, Wormhole, RTT, Clustering, NS-2*

1. INTRODUCTION

The popularity of wireless network is increase day to day. The increased popularity responsible for reliable and secured combination of data over the network. The mobility and dynamic infrastructure of wireless network invites some security threats. Encounter of security threats various malicious attack are involved such as black hole attack, worm hole attack, sink attack and many packet -based attacks. These attacks theft the data and degraded the performance of wireless network [1-2]. In this paper basically focus on worm hole attack detection. The process of security threats divide in tow section active and passive attack. A functioning assault endeavors to modify or pulverize the information being traded in the system, subsequently disturbing the typical working of the system. It can be arranged into two classifications outside assaults and inward assaults. Outside assaults are completed by hubs that don't have a place with the system [7-9]. These assaults can be forestalled by utilizing standard security components, for example, encryption methods and firewalls. Interior assaults are done by bargained hubs that are a piece of the system. Since the assailants are as of now part of the system as approved hubs, inner assaults are more serious and hard to recognize when contrasted with outer assaults. An uninvolved assault does not disturb legitimate task of the system. The assailant noses the information traded in the system without changing it. Here, the necessity of classification can be disregarded if an assailant is likewise ready to translate the information accumulated through snooping[4]. Location of detached assaults is extremely troublesome since the activity of the system itself does not get influenced [3]. In a wormhole assault, two aggressor hubs join. One aggressor hub gets bundles at one point and "passages" them to another assailant hub by means of a private system association, and after that replays them into the system.

Wormhole assault is a hand-off-based assault that can upset the steering convention [10-11]d thusly disturb or breakdown a system and because of this reason, this assault is not kidding. For the prevention and detection of wormhole attacks various algorithms and methodology are proposed. In the consequence of detection of wormhole attack proposed the K-distance based algorithm for wormhole attack detection[7-8]. The K-distance formula derived the position of normal node and wormhole node during the process of communication. The rest of paper organized as section II. Process model of wormhole. In section III. Proposed algorithm. in section IV simulation of network and finally conclude in section V.

2. PROCESS OF WORMHOLE

In a wormhole attack, two attacker nodes join. One attacker node receives packets at one point and “tunnels" them to another attacker node via a private network connection, and then replays them into the network.

Wormhole attack is a relay-based attack that can disrupt the routing protocol and therefore disrupt or breakdown a network and due to this reason, this attack is serious. We can use 4 steps to explain about a general wormhole attack[10, 12].

1. An attacker has two trusted nodes in two different locations of a network with a direct link between the two nodes.

2. The attacker records packets at one location of a network.

3. The attacker then tunnels the recorded packets to a different location.

4. The attacker re-transmits those packets back into the network location from step 1.

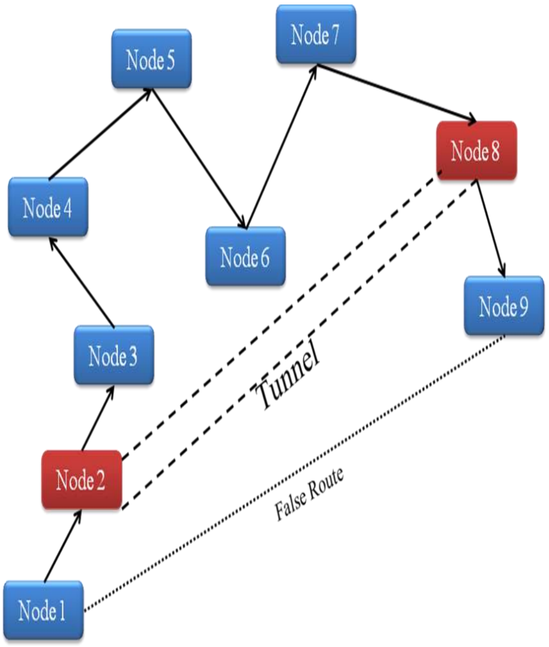

Figure 1: Scenario of Wormhole.

Figure(1) shows the simple worm hole in the network. Here node 2 and node 8 create the tunnel in order to work as a malicious node. Both nodes give the illusion to another node that there is a shortest path. But this shortest path does not exist and attack can easily perform by the attacker[5-6].

There are three types of wormhole attacks are available. There are classified based on its Nodes. There is open wormhole attack, half open wormhole attack and closed wormhole.

Pen Wormhole Attack: In this type of attack both nodes are available in the network in order to complete the communication in the network. Here both nodes can change the data as well as show them self in route discovery path.

Half Open Wormhole Attack: In this type of attack one node is open in network in order to spoil the integrity of data.

Closed Wormhole Attack: When the tunnel has formed then both node hide then self from the network but act for modifying the data. They show that the shortest path to the send the data.

3. PROPOSED ALGORITHM

For the detection of wormhole attack in wireless network used k-distance based function. The k-distance based function estimate the group of near nodes based on same number of request and creates cluster. The formation of cluster based on the number of request and responded processes of communication. The process of algorithms describes here

k-distance(p): The distance between a node point and its kth node neighbor—kth-NN).

Reachability distance (reach-dist) of a node point p with respect to another node point o

wormholenode - dist$_k$ (p, o) =

$$= \min \{k - distance(0), d(p, o)\} \quad (1)$$

where d *(p, o)* is the euclidean distance between *p* and *o.*

minimum RTT of k distance pp

$$RRT_k(p) = \left(\frac{1}{k}\sum_{0\in N_{(p,k)}} reach - dist_k(p,o)\right) \quad (2)$$

Where $N_{(p,\,k)}$ is the set of k same request *p*

Worm hole detection

$$whd(p) = \frac{1}{k}\sum_{0\in N_{(p,k)}} \frac{rrt_k(o)}{rrt_k(p)} \quad (3)$$

Algorithm Steps

N_{of} = normal node
W_{hd}=wormhole detection
Input: set of requests point
P ={ p_n, … … … , p_n }
Cluster of *m (empty b:c = m - b)*

Output: set of *whd ={ whd (p_1), … … … , nof p_n } value*

```
i ← 0; {step}
for all $p_t \in P$ do
    nof ($p_t$) ←normal node Insertion ($p_t$)
    if normal node is =b then
        $C^i \leftarrow \left\{p_{i\frac{b}{2}+m} I\ m \in \left\{1, \dots, \frac{b}{2}\right\}\right\}$
Compute $k - distance(v_j^i), rrt(v_j^i), nof(v_j^i)$
    end for
    if I > 0 then
        compute   k-distance($z_j$)LOF($z_j$)
similarly
        worm hole node detected
        Update k-point distance p
    end if
    i ← i + 1 ;
    end if
    end for
    return whd.
```

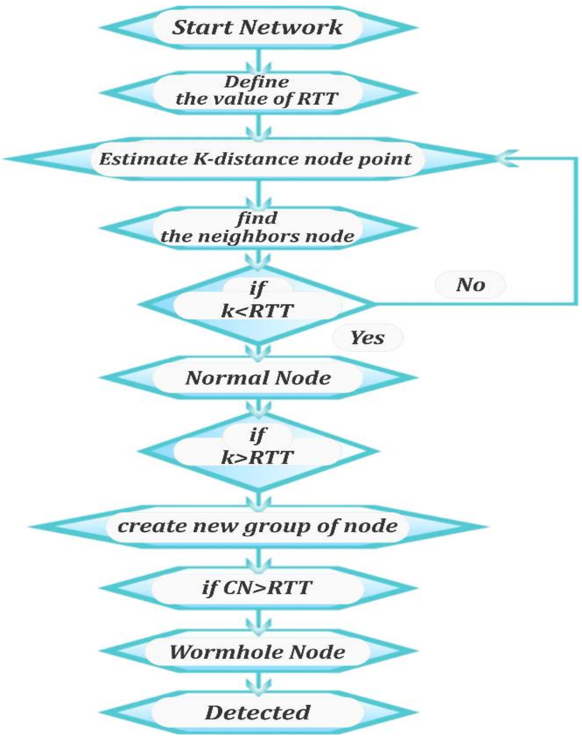

Figure 2: Proposed model of worm hole detection based on k-distance and RTT.

4. SIMULATION AND EXPERIMENTAL RESULT

In this section discuss the process of simulation and analysis of result. The proposed algorithm is simulated in NS-2 software. The NS-2 Software is well known network simulator for wireless network.

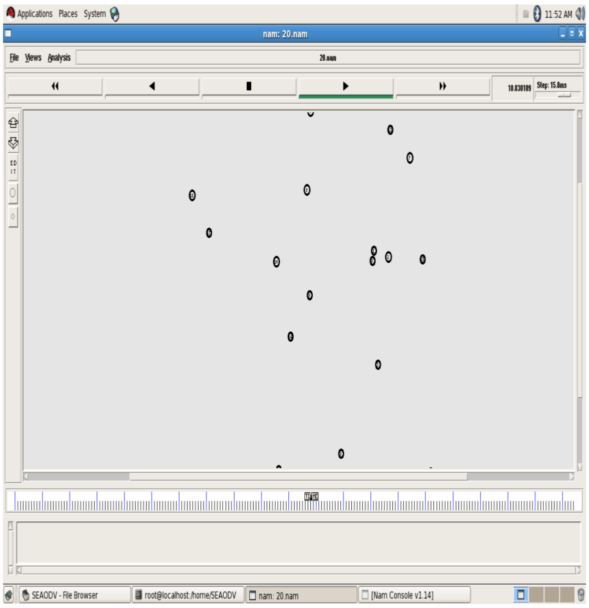

Figure 3: Simulation Scenario of Modified CDF Scheme on Pause Time 30sec.

Above figure shows that packet behavior in the normal mode to the attacking mode in normal mode the rate of packet receiving and transmission is maximum and the rate of attack increase the drop rate of packet is decrease.

Table 1: Simulation Parameters.

Parameter	Value
Simulation Duration	50, 100, 150, 200Sec.
Simulation Area	1000*1000
Number of mobile nodes	10, 20, 30, 40, 50
Traffic Type	Cbr(udp),
Packet Rate	4 packet/sec.
Abnormal Node	Variable
Host Pause Time	10 Sec.

We recreate our strategy in NS-2 with help of OTCL and TCL reenactment script record, now assessment of execution of these changed plans we utilized standard parameter of ad-hoc system.

Packet Delivery Ratio

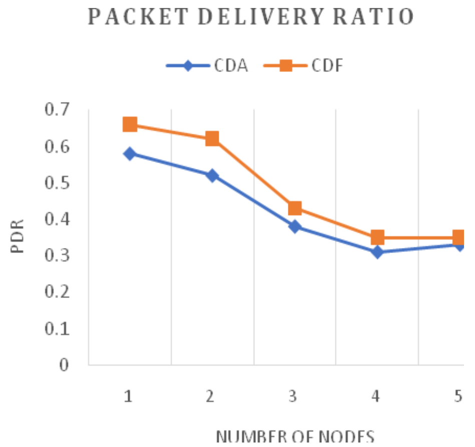

Figure 4: Packet Delivery Ratio vs Speed of Nodes.

Figure shows the packet delivery ratio for CDA and CDF. We can observe from the figure that Both CDA and CDF improves the packet delivery ratio than CDA.

Normalized Routing Load

Figure it can be observed that CDA has more routing overhead compared to both the CDF.

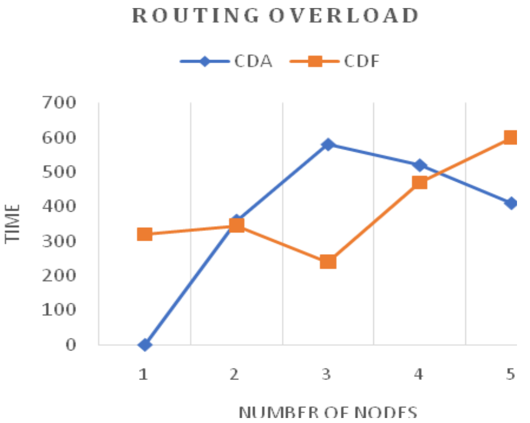

Figure 5: Normalized Routing Load Vs Speed of Nodes.

Both the way misfortune delicate variations of CDA does not handle the RREQ in the event that it is having vast way misfortune, that will decrease the directing burden in both the variations. The CDA does not have stable course which expands the course disclosure. Expanded course revelation acquires all the more directing overhead.

Average End to End Delay

From Figure we can observe that CDA achieves reduction in average end to end delay. This can happen because CDA has the minimum hop route and CDF has a route with higher no of hops than CDA.

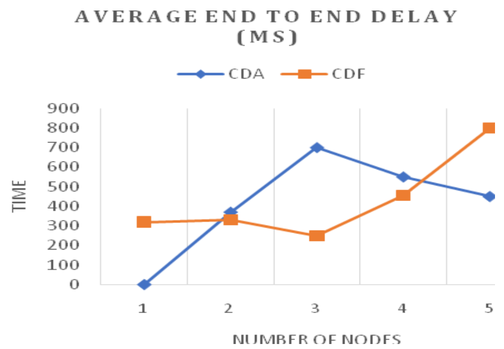

Figure 6: Average End to End Delay Vs Speed of Nodes.

CDA has least no of jumps in this way, there will be less time spent in handling the information parcels. The reality of the matter is that both CDF gives stable course at the same time, they discover a course with expanded no of jumps contrasted with CDA which will build the End to End postpone contrasted with CDA. The expanded End to End defer of both CDF is considered as an exchange off of our proposed work i.e. the value we are paying to accomplish the steady way.

Throughput

CDA has a better end to end delay which will help to improve the throughput of the network. Reduced throughput of CDF compared to CDA suggests that throughput is a trade-off to achieve stable route.

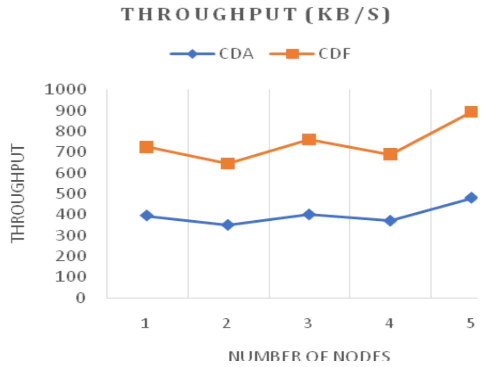

Figure 7: Throughput Vs Speed of Nodes.

5. CONCLUSION & FUTURE WORK

In this paper proposed k-distance based algorithm for the detection of wormhole node in wireless network. The proposed algorithm considers two distance point one is near node as same group and other is fear node with different group. the near and fear group creates number of cluster and validate their position of node. The position of node decides the normal node and malicious node in wireless network. The proposed algorithm simulates in NS-2 simulator and measured some parameters such as PDR, normalized load and network throughput. The proposed algorithm compares with CDS algorithms. The CDS algorithms stans for centralized distribute system for wormhole detection.

REFERENCES:

[1] Shiyu Ji, Tingting Chen, Sheng Zhong "Wormhole Attack Detection Algorithms in Wireless Network Coding Systems" IEEE Transactions On Mobile Computing, Vol-14, 2015.pp 660-674.

[2] Amit Kumar "A Parameter Estimation Based Model for Worm Hole Preventive Route Optimization" International Journal of Computer Science and Mobile Computing, 2015. pp 80-85.

[3] MahaAbdelhaq, Raed Alsaqour, Mohammed Al-Hubaishi, Tariq Alahdal, Mueen Uddin "The Impact of Resource Consumption Attack on Mobile Ad-hoc Network Routing" IEEE, 2013. Pp 376-381.

[4] Moutushi Singh, Rupayan Das "A Survey of Different Techniques for Detection of Wormhole Attack in Wireless Sensor Network" International Journal of Scientific & Engineering Research, Vol-3, 2012.pp 1-6.

[5] Badran Awad, Tawfiq Barhoom "BT-WAP: Wormhole Attack Prevention

Model in MANET Based on Hop-Count" IJARCCE, 2015. Pp 600-606.

[6] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks" ACM, 2005. Pp 46-57.

[7] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks" IEEE, 2008. Pp 343-348.

[8] Shraddha S. Mahajan, Dr. Hitendra D. Patil "Wormhole Detection and Prevention in MANET: A Review" IJCSMC, 2015. Pp 980-984.

[9] Issa Khalil, Saurabh Bagchi, Ness B. Shroff "MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks" Elsevier ltd. 2007, pp 344-362.

[10] Tassos Dimitriou and Athanassios Giannetsos "Wormholes no more? Localized Wormhole Detection and Prevention in Wireless Networks" 2012.Pp 1-14.

[11] J. Eriksson, S. V. Krishnamurthy, M Faloutsos "Truelink: A practical countermeasure to the wormhole attack in wireless networks" 2006, pp 75–84.

[12] W. Wang, B. Bhargava, Y. Lu, X. Wu "Defending against wormhole attacks in mobile ad hoc networks: Research articles" Wireless. Communication Mobile Computer 2006, pp 483–50.