International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 6, November - December 2015 ISSN 2278-6856

Novel Method for the Detection of Wormhole Attack in Delay Tolerant Network

Jyothi D G[1], Ajay Kumar S N[2], Dr.Chandra shekara S N[3]

[1]Department of Computer Science and Engineering, Bangalore Institute of Technology
Bangalore - 560004, Karnataka, India

[2]Department of Computer Science and Engineering, Bangalore Institute of Technology
Bangalore - 560004, Karnataka, India

[3]Department of Computer Science and Engineering , SJCIT,
Chickballapura, Karntaka,INDIA

ABSTRACT
Wireless communication faces several security risks. In this paper, we are concerned of a particularly severe security attack that affects the Delay Tolerant Networks routing protocols, it is called the wormhole attack. The algorithm uses the local connectivity information to look for forbidden substructures in the network connectivity graph. Our proposed methodology is wholly localized and it does not use any special hardware or location information of the nodes, making this technique universally applicable. The objective of this paper is to develop a methodology to detect the presence of malicious nodes, causing forbidden structure in the network, using only local connectivity information.

Key words: wormhole attack, Delay Tolerant Network, Unit Disk Graph.

I. INTRODUCTION

With the quick progress in wireless technology, Ad hoc networks have developed into many forms. These wireless networks operate in the license free frequency band and does not require any investment in infrastructure, making them adopt widely in military and few commercial applications. On the other hand, there are many issues yet unsolved in ad hoc networks; one of the major concerns is security in the network. Ad hoc networks are vulnerable to various security attacks due to numerous reasons; the absence of physical infrastructure, wireless means of communication between the nodes in the network, restricted physical Protection, and the absences of a centralized monitoring system or management, and the resource constraints of mobile nodes.

In this paper our focus is on a particularly destructive form of attack, called wormhole attack in Delay Tolerant Network. Here, the adversary connects two distant points in the network directly using a lower latency connection called the wormhole link. The wormhole link between two nodes can be created by a various means, e.g., by using a direct wired link technology or a long-range direct wireless transmission in a unique band. The end-nodes of the wormhole link are equipped by radio transceivers compatible with the network. When the wormhole link is established between colluding nodes, the adversary captures packets in transmissions in the network on one end of the link, passes them through the wormhole link and relays them at the another end of the link.

A.Delay Tolerant Network

Delay Tolerant Networking (DTN) is communication networking models that enable communication in the networking environment where there may not be an end-to-end path, communication opportunities between the nodes may be rare and their communication interval can be very high and its information is not even known beforehand. Routing data packets in this kind of the situation is quite different when compared to other traditional communication networking models. A Delay Tolerant Network is collection of computing systems in the network, called nodes. The one-way links may connect few nodes together within each other's range. These links may go up and down over the time, due to nodes constant mobility, connection failures, connection duration or other events. When the communication link is up, the source node gets an opportunity to transmit data to the node on the other end. In the DTN literature this opportunity is called contact. More than one contact may be possible between the pair of nodes. For example, the node might have two types communication interface a high-performance, expensive connection interface and a low-performance, inexpensive connection interface that are used concurrently for communication with the same destination.

B.The Wormhole Attack

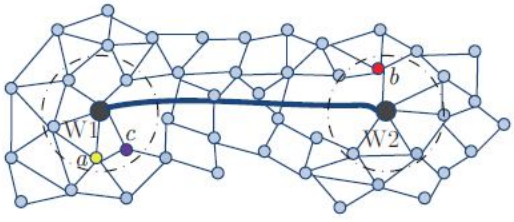

Fig. 1 Deployment of Wormhole Attack

In a wormhole attack the attacker connects two compromised nodes in the network that are placed far

away from each other using a low-latency high speed link. Then, one malicious node records in the one end and tunnels data packets to another colluding node which replays them in the other end. Such an action can give impression to the nodes that are within the transmission range of the malicious nodes that they are the neighbors of some other nodes in realty which are actually far away from them. This result, the compromised end nodes of the wormhole link may draw more routes and packets through them. Then they can launch additional attacks. For example, they can carry out selective dropping of data packets; record the data for further analysis of traffic, and so on.

Wormhole Attack Modes: Wormhole attacks can be launched using several different methods

1) Wormhole through Tunneling: In this method a compromised node at one part in the network, captures the RREQ (route request) packet. It tunnels it to a second colluding node at a distant location in the network near the destination. The second node then re-broadcasts the RREQ packet. The neighbors around the second colluding node receive the RREQ packets with lesser route length and drop all the legitimate requests that may come afterward on legitimate multi hop routes. The result is that the routes between the source and the destination node go through the two colluding nodes that will be said to have formed a wormhole between them.

2) Wormhole with High Transmission Power*:* Another technique is the use of high transmission power. In this method, when one malicious node gets a RREQ, it broadcasts the request packet at very high power intensity; a capacity which is does not exist in other nodes in the network. Any node which hears this high intensity broadcast rebroadcasts it towards the destination node. By this mode, the malevolent node increases its possibility to be in the routes established among the source and the destination even without the involvement of a colluding node.

3) Wormhole by Protocol Manipulation: A wormhole attack can also be done through protocol Manipulation. During forwarding the RREQ packets, the nodes usually back off for a random duration of time prior to forwarding to decrease MAC layer collisions. A malicious node can construct a wormhole by merely not complying by the protocol and broadcasting by without backing off. The reason is to let the RREQ packet it forwards arrive first at the destination node.

C.Opportunistic Network Environment

Opportunistic Network Simulator (ONE) is specially designed for Delay Tolerant Network (DTN). The main functions of the ONE simulator are the modeling of node movement, inter-node contacts using various interfaces, routing, message handling and application interactions. Result collection and analysis are done through visualization, reports and post-processing tools. The nodes are grouped in node groups and a one group shares a set of common parameters such as message buffer size, radio range and mobility model. Since different groups can have different configurations. Node movement is implemented by movement models. These are either synthetic models or existing movement traces. Connectivity between the nodes is based on their location, communication range and the bit-rate. The routing function is implemented by routing modules that decide which messages to forward over existing contacts. Finally, the messages themselves are generated either through event generators that generate random traffic between the nodes, or through applications that generate traffic based on application interactions. The messages are always unicast, having a single source and destination host inside the simulation world.

The ONE can be run in two different modes: batch and GUI. The GUI mode is especially useful for testing, debugging and demonstration purposes and the batch mode can be used for running large amount of simulations with different set of parameters. If there is no need for real-time visualization, it is more efficient to run simulations in the batch mode. ONE is able to visualize results of the simulation in two ways: via an interactive Graphical User Interface (GUI) and by generating images from the information gathered during the simulation.

II. RELATED WORK AND ITS DRAWBACK

In **[1]** the authors used the location information from GPS system into the transmitted packets. The receiving node uses the location information to confirm whether there is a wormhole attack. This is also called as the *geographical leash* approach and requires only loosely synchronized clocks. But, this technique suffers when there are circumstances where obstacles prevent communication between two nodes that would otherwise be in the transmission range. The authors also proposed a temporal leash method where a sending node includes the time information in the packet and the receiving node compares the time at which it receives that packet to see if the packet has traveled beyond a threshold based on transmission time. However, this temporal leash approach requires tight clock synchronizations, and thus it is hard to achieve with resource constrained nodes.

In **[2]** proposed the secure tracking of node encounters (SECTOR) scheme to prevent wormhole attacks. In SECTOR the Mutual Authentication with Distance Bounding (MAD) protocol enabled nodes to find their true neighbors by determining their mutual distances when they encounter one another. MAD used bit exchanges between each pair of encountered nodes: one node first sent out one bit, which is considered a challenge, and then another node responded with one bit immediately after receiving the challenge. By measuring the time between sending out a challenge and receiving the response, the first node can compute an upper bound of the distance between these two nodes and then check if this distance violates any physical constraints (e.g., the speed of light). The disadvantage of this method is that it needs special hardware for measuring timing with nanosecond precision.

In **[3]**, the authors introduced directional antennas into a network and proposed a directional neighbor discovery protocol to prevent wormhole attacks. With directional antennas, the region around a node is divided into zones. Their neighbor discovery method is based on the fact that only nodes that are located in zones, which are in the opposite direction, can be true neighbors in legal networks. Thus, in this method the neighbor discovery protocol only allows nodes that are in certain zones to accept each other as neighbors, and this strategy can avoid accepting most of the fake neighbors masqueraded by the wormhole link.

Even though this method greatly diminishes the threat of wormhole attacks, it requires all nodes to use directional antennas.

In **[4]** connectivity information is used to detect the presence of wormholes. However, the method proposes to detect by changing the range of communication of the nodes. This variation in communication range affects the normal operation of communication.

III. PROPOSED METHODOLOGY

A. Unit Disk Graph Model

In unit disk graphs (UDG) each communicating node is modeled as a 2 dimensional disk of unit radius in the plane, It represents the communication range of the node with an Omni-directional antenna. All the nodes located within the disk are neighbors of the node. UDGs have been used for long time to construct an idealized model of multi-hop wireless networks. If the resulted connectivity graph is not in valid UDG embedding in the plane, then it can be deduce that the wormhole must be present in the network. This non-valid embedding can occur when wormhole attack creates long-distance links (longer than unity) which will not exist in a normal UDG model. On the contrary, if the observed connectivity graph does declare a valid UDG embedding, then *any* algorithm based on connectivity information will produce a negative output 'wormhole attack'. In such a situation, even if the wormhole link is present, it is not distinguishable from a legal link in the embedded UDG model. In the lack of any further information, this UDG embedding has to be taken as the ground truth. This situation may come, when wormhole links are short then unit distance and thus appear no different than a regular link in UDG. There can also be situation like, when the link is very long, but lack of enough node density prevents wormhole detection. The fundamental idea in our detection algorithm is to search for graph substructures that do not permit a unit disk graph embedding, thus which cannot be present in a legal connectivity graph.

B. Disk Packing

Packing argument – Inside a fixed region, it is not possible to pack too many nodes without having edges in between them. Thus the forbidden substructures we look for are those that actually violate this packing argument.

The packing number is denoted by $p(S, r)$, which represents the maximum number of nodes inside a region S such that every pair of nodes is strictly more than inter distance r away from each other. A disk of radius R denoted by $D_R(u)$,centered at position u. To simplify the notations unit disk is denoted by D. A unit disk can contain at most 5 nodes, whose pair-wise distances between each other are strictly more than 1. Thus $p(D, 1) = 5$.

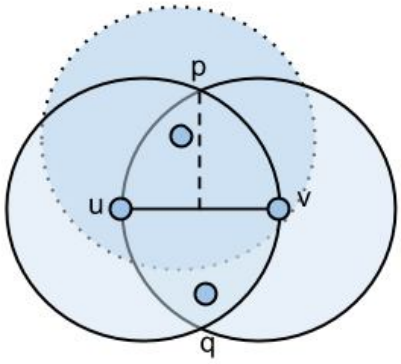

Fig. 2 One can only pack at most two nodes inside a Lune with inter-distance more than 1.

Given two disks of radius R placed at u, v with inter distance r away, define by Lune the intersection of the two disks, $L(r,R) = D_R(u) \cap D_R(v)$. When $R = r = 1$, the line segment uv divides the Lune into two parts, the upper and lower ones. The two intersections of the two unit circles centered at u, v are denoted p, q respectively. Denote by w the midpoint of segment uv. $|pw| = \sqrt{3}/2 < 1$. It is not hard to see that inside the upper half of the Lune one cannot place two nodes with their distance strictly larger than 1. Indeed, for any node x in the upper half of L, $|xv| \leq 1$, $|xu| \leq 1$, $|xp| \leq 1$. Thus there can only be two nodes inside L with inter distance larger than 1.

C. Forbidden Substructure For Wormhole Detection

The disk packing lemma defines the forbidden substructures for the unit disk graphs. A wormhole connects all nodes in region A with all the nodes in region B. Thus it results in two independent (i.e., non-neighbor) nodes in region A, say, x, y, that have three common neighbors p, q, r in region B that are independent. This creates a forbidden structure, because in any valid UDG embedding of the connectivity graph the three common neighbors must be within the intersection of disks centering x, y. given that they are independent, their pair wise distance must be more than 1.

D. Steps Of The Wormhole Detection

1) Each node u determines its 2-hop neighbor list, $N_2(u)$, and executes the following steps for each non-neighboring node v in $N_2(u)$.

2) Node *u* determines the set of common *2*-hop neighbors with *v* from their *2*-hop neighbor lists. This is $C_2(u, v) = N_2(u) \cap N_2(v)$. This can be determined by simply exchanging neighbor lists.
3) Node *u* determines the maximal independent set of the sub-graph on vertices $C_2(u, v)$
4) If the maximal independent set size is equal or larger than *3*, node *u* declares the presence of a wormhole.

IV. SIMULATION

The simulation of this experiment has been conducted using Opportunistic Networking Environment (ONE) Simulator, ONE simulator specifically designed for evaluating DTN routing and application protocols. It allows users to create scenarios based upon different synthetic movement models and real-world traces and offers a framework for implementing routing and application protocols. Interactive visualization and post-processing tools support evaluating experiments and an emulation mode allows the ONE simulator to become part of a real-world DTN test bed. The simulation has been carried out using below mentioned parameters.

Parameter	Values
Simulation Time	3000 sec
World size	4500,3400
Router	Epidemic router
Buffer size	5mb
Wait time	0,120
Interface	1
Speed	0.5,1.5
No of Wormhole	1
Movement Model	ShortestPathMapBasedMovement

A. Network Under Normal Condition

The below figure is an initial view of the simulation environment when we run the simulation. The circles colored green represent the transmission range of nodes and the nodes itself are represented with labels (colored blue). The thin grey lines in the background represent the paths in the map that we have used for node movement. Each node has a predefined path to be followed during the simulation. Simulation window shows the network behavior under normal condition.

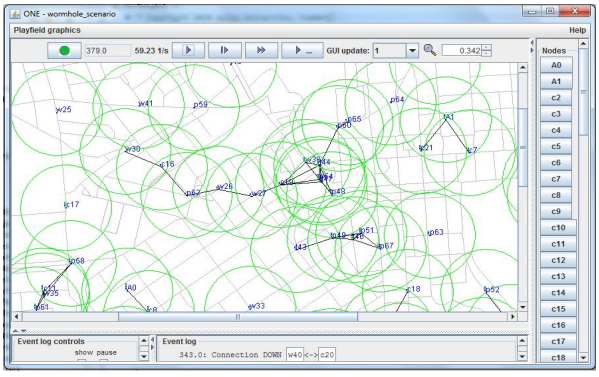

Fig. 3 Simulation window shows the Network under normal condition.

B. Network Under Wormhole Attack

By using the ONE simulator we are creating wormhole attack environment. Here the nodes A0 and A1 are the wormhole nodes. When there is a Wormhole attack, the neighbors of node A1 will be the neighbors of A0 and vice versa. There will be a link exist between the neighbors of these two wormhole nodes. As we are using the Epidemic routing protocol, all the nodes of the network receive the copy of the packets. The sender node flooding the networks by the packets until the all nodes has the copy of the packet. Here the Data messages pass through the wormhole link.

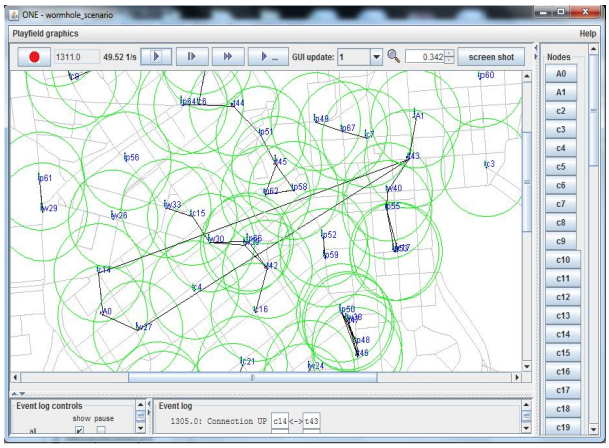

Fig. 4 Simulation window showing the Wormhole attack in the Network.

C. Wormhole Detection Scenario With Result

The below figure shows the scenario, where the wormhole attack is detected. The console output is also shown in the figure. In this scenario the detection algorithm runs on the two nodes C34 and A1. Which are non-neighbor nodes but the result shows it has 3 common independent neighbors i.e., T104, W86, W85. This cannot happen in normal situation and it violates disk packing lemma so the algorithm detects the wormhole presence in the network.

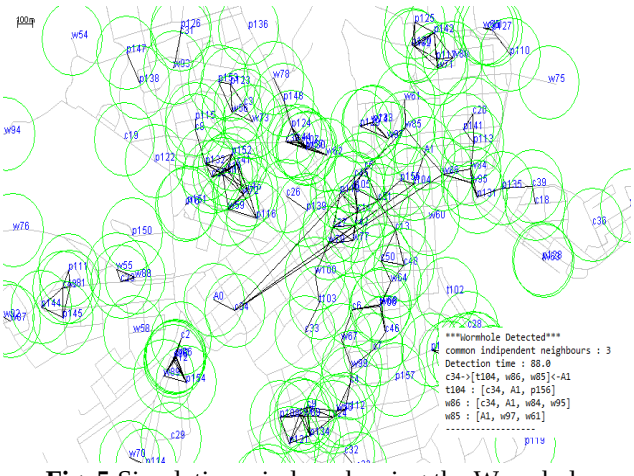

Fig. 5 Simulation window showing the Wormhole detection with the result.

D.Experimental Results

In the simulation, we observed that the increase in node density results in the faster detection of a wormhole attack, as it results in the increase formation of more forbidden structures. Furthermore, the detection probability increases as the time increases. The detection probability doesn't depend on the node density, on an average the detection probability increases in same rate on varied node densities.

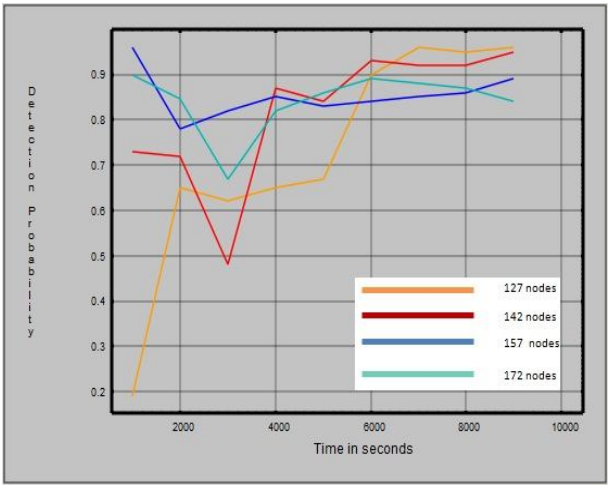

Fig. 6 Graph showing detection probability vs. detection time

The following graph shows the detection time decreases as the node density increases. Here Detection time is observed by varying the node density. The result shows detection rate is faster when number of nodes increases. We are detecting the wormhole based on connectivity information, the number of links increases between the nodes increasing rate of forbidden structure formation, the system will detect the presence of wormhole attack. In this graph, x-axis represents the Number of nodes and y-axis represents the Detection time in seconds.

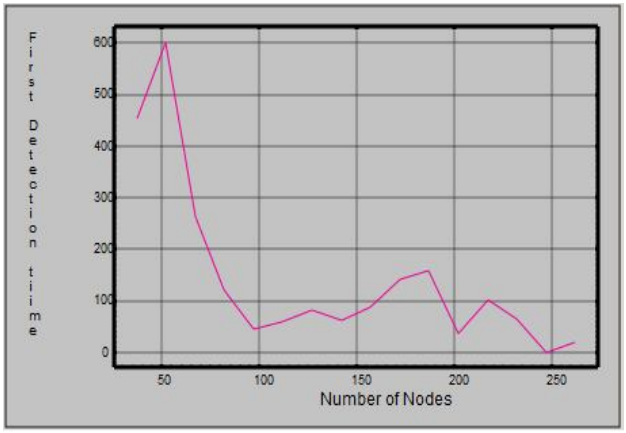

Fig. 7 Graph showing Detection Time in seconds vs. Number of nodes

V.CONCLUSION

In this paper we propose an algorithm for the detection of wormhole attack in the Delay Tolerant Networks. First we created a wormhole attack environment, i.e. how the system will behave in case of wormhole attack, and then we used the wormhole detection scheme to check the presence of wormhole attack in the network. In our system, we are detecting the wormhole attack by only using the connectivity information. The algorithm used for detection is simple, localized, and is universal to node distributions. No extra hardware is used. Our proposed system works efficiently when the density of the node is high. When the density of nodes is sparse proportionately the detection time increases.

REFERENCES

[1]. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, 2003.

[2]. S. Capkun, L. Buttyan, and J. P. Hubaux, "Sector: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks," Proc. ACM SASN, 2003.

[3]. L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," Network Distrib. Sys. Sec., 2003.

[4]. Yanzhi Ren , Mooi Choo Chuah , Jie Yang , Yingying Chen, Detecting wormhole attacks in delay-tolerant networks, IEEE Wireless Communications, v.17 n.5, p.36-42, October 2010.