ISSN:0975-9646

A Survey on Wormhole Attack Detection in Wireless Network

Haritima Shrivastava
Department Of Computer Science Engineering,Software Engineering Bhopal,RGPV University Bhopal,India

Sandeep Pratap Singh
Department Of Computer Science &Engineering,OIST Bhopal RGPV OIST University, Bhopal, India

Abstract- Security and authentication of wireless communication is big issue in current scenario. For the improvement of security and authentication used various method and technique such as coding system, threshold based system, distributed algorithm and centralized algorithm in wireless network. These entire algorithms have certain limit in terms of performance and network overhead. In this paper discuss the algorithms for the detection of wormhole attack detection. The wormhole detection is critical task in wireless network, due to dynamic infrastructure and mobility of node. This paper presents a review of wormhole attack in mobile ADHOC network.

Keywords: - wireless network, wormhole

I. INTRODUCTION

A collection of self-configuring mobile node without any communications network is called The Mobile Ad-hoc Network (MANET) is [4]. In a Mobile ad-hoc network every nodes is connect by wireless radio interface using wireless links so every node can free to move without any connection and without any rhyme with capability of variable links with other devices again and again[6]. Because of it is a multi-hop process, the partial communication range of energy constrained portable nodes and thus each tool in network topology acts as a router. Using dynamic nature of network topology the routes changes very fast and frequent and so the efficient routing protocols plays important roles in handling it. They should be capable to ensure the delivery of packets safely to their destinations. MANETs are also capable of handling topology changes and malfunctions in nodes through network reconfigurations. Examples include on-the-fly conferencing applications, networking intelligent sensors or devices etc. Interest in such dynamic wireless networks is not new [1]. It times back to the seventies, when the U.S. Defense Research Agency, DARPA worked on PRNET and SURAN projects. They supported automatic route set up and maintenance in a packet radio network with adequate mobility. Interest in such networks has recently grownup due to the common availability of wireless communication devices that can connect laptops and palmtops and operate in license free radio frequency bands (such as the Industrial-Scientific- Military or ISM band in the U.S.). In an interest to run internetworking protocols on ad hoc networks, a new working group for Mobile, Ad hoc Networking (MANET) has been formed inside the Internet Engineering Task Force (IETF), whose charter includes developing a framework for running IP based protocols in ad-hoc networks. Interest has also been partly driven by the recent IEEE standard 802.11 that include the MAC and physical layer specifications for wireless LANs without any fixed infrastructure [10]. Routing protocols in packet-switched networks traditionally use either link-state or distance-vector routing algorithm. Both algorithms allow a host to find the next hop neighbor to reach the destination via the “shortest path.” The shortest path is usually in terms of the number of hops; however, other suitable cost measures such as link utilization or queuing delay can also be used. Such shortest path protocols have been successfully used in many dynamic packet switched networks. Prominent examples include use of link state protocol in OSPF (Open Shortest Path First) [9] and use of distance vector protocol in RIP (Routing Information Protocol) for interior routing in the Internet. Even though, any such protocol would, in principle, work for ad hoc networks, a number of protocols has been specifically developed for use with ad hoc networks. The primary motivation is that the shortest path protocols, either link state or distance vector, take too long to converge and have a high message complexity. Because of the limited bandwidth of wireless links, message complexity must be kept low. Also, potentially rapidly changing topology makes it important to find routes quickly, even if the route may be sub optimal. Several new ad hoc routing protocols have been developed with this basic philosophy. Section-II gives the information of wormhole attack. In section III discuss the related work. In section IV discuss the discuss detection problem of wormhole technique. Finally, in section V conclusion and future scope.

II. WORMHOLE ATTACK

In a wormhole attack, two attacker nodes join together. 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 [5] 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. An attacker has two trusted nodes in two different locations of a network with a direct link between the two nodes. The attacker records packets at one location of a network. The attacker then tunnels the recorded packets to a different location. The attacker re-transmits those packets back into the network location from.

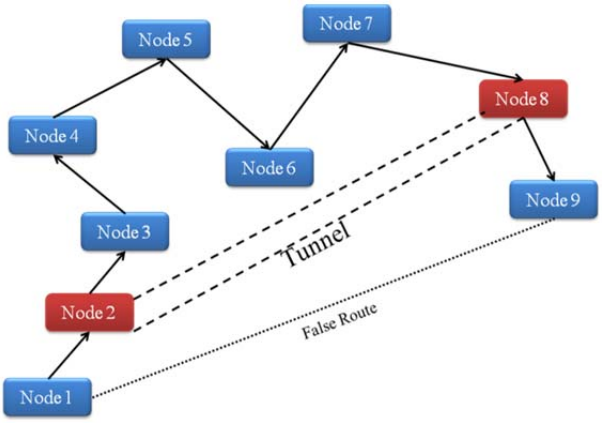

Figure:1: Example of Wormhole.

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.There are three types of wormhole attacks are available [9]. There are classified on the basis of its Nodes. There are open wormhole attack, half open wormhole attack and closed wormhole.Open 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.According to whether the attackers are visible on the route, wormholes can be classified into three types [11]: closed, half open, and open. The examples that include two malicious nodes are shown in Figure 2, consider M1 and M2, represent the malicious nodes. S and D represent the good nodes as source and destination, and A, B etc. as the good nodes on the route. The nodes between the curly-braces ("{}") are the nodes which are on the path but invisible to S and D because they are in a wormhole. In the wormhole attack "closed," means, "start from and include," and "open" means, "start from but not include" [12]. In (a), M1.and M2. tunnel the neighbor discovery beacons from S to D and vice versa, for this reason S and D assume that they are direct neighbors to each other. In Figure(b), M1 is a neighbor of S and it tunnels its beacons through M2 to D, Only one malicious node is visible to S and D In an open wormhole, both attackers are visible to S and D as shown in (c) .

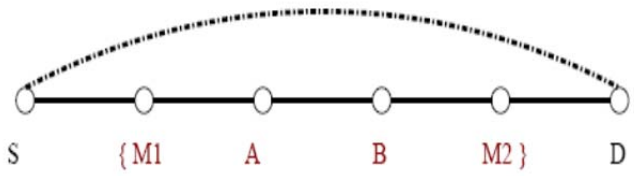

Figure 2: Closed wormhole attack

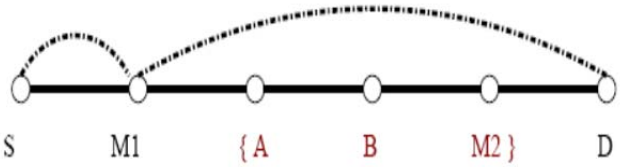

Figure 3: Half open wormhole attack

III. Related Work

In this section discuss the detection and prevention process of wormhole attack in mobile adhoc network. The dynamic infrastructure and node mobility invites the various types of attack in network. In the process of detection and prevention various techniques is proposed by various authors and researcher. Some work discuss in this section for the prevention and detection of wormhole attack.

[1] In this paper, we quantify wormholes' devastating harmful impact on network coding system performance through experiments. We first propose a centralized algorithm to detect wormholes and show its correctness rigorously. For the distributed wireless network, we propose DAWN, a Distributed detection Algorithm against Wormhole in wireless Network coding systems, by exploring the change of the flow directions of the innovative packets caused by wormholes. We rigorously prove that DAWN guarantees a good lower bound of successful detection rate. We perform analysis on the resistance of DAWN against collusion attacks. We find that the robustness depends on the node density in the network, and prove a necessary condition to achieve collusion-resistance. DAWN does not rely on any location information, global synchronization assumptions or special hardware/middleware. It is only based on the local information that can be obtained from regular network coding protocols, and thus the overhead of our algorithms is tolerable. Extensive experimental results have verified the effectiveness andthe efficiency of DAWN.

[2] In this paper and adaptive communication model is defined for wormhole infected mobile network. The presented model has provided the optimized parameter adaptive communication. Results shows that the work has improved the communication throughput and reduced the loss. This network for is defined with specification of relative problem so that the adaptive communication is obtained from the work. The protocol is also defined with specification of the communication parameter, architecture adaptive utilization and the route formation. The network suffers from various issues shown in the network. The first and foremost challenge to the network is the its mobility. The mobiles nodes at different speed increase the interruption during the communication so that the communication loss is expected.

[3]In this research paper work, some modifications has been done in AODV routing protocol todetect and remove wormhole attack in real-world MANET. Wormhole attack detection and prevention algorithm, WADP, has been implemented in modified AODV.Also node authentication has been used to Detectmalicious nodes and remove false positive problem that may arise in WADP algorithm. Node authentication not only removes false positive but also

helps in mapping exact location of wormhole and is a kind of double verification for wormhole attack detection .Simulation results provesthe theory.

[4] In this paper, we present a countermeasure for the wormhole attack, called MOBIWORP, which alleviates these drawbacks and efficiently mitigates the wormhole attack in mobile networks. MOBIWORP uses a secure central authority (CA) for global tracking of node positions. Local monitoring is used to detect and isolate malicious nodes locally. Additionally, when sufficient suspicion builds up at the CA, it enforces a global isolation of the malicious node from the whole network. The effect of MOBIWORP on the data traffic and the fidelity of detection is brought out through extensive simulation using ns-2. The results show that as time progresses, the data packet drop ratio goes to zero with MOBIWORP due the capability of MOBIWORP to detect, diagnose and isolate malicious nodes. With an appropriate choice of design parameters, MOBIWORP is shown to completely eliminate framing of a legitimate node by malicious nodes, at the cost of a slight increase in the drop ratio. The results also show that increasing mobility of the nodes degrades the performance of MOBIWORP.

[5] In this paper, a new model is developed for detection and prevention of wormholes based hop-count metric which we call it BT-WAP. BT-WAP effectively and efficiently isolates both wormhole node and colluding node. Our model allows the evaluation of node behavior on a pre-packet basis and without the need for more energy consumption or computation-expensive techniques. We show via simulation that BT-WAP successfully avoids misbehaving nodes. It is found that the BT-WAP model achieves an acceptable detection rate about 99.7% and a detection accuracy rate 98.4%. which makes BT-WAP an attractive choice for MANET environments.

[6] In this paper, we propose a new idea for neighbor discovery process by introducing prehandshakingstrategy. A prehandshaking strategy will analyze the activities of neighboring node and help to reduce collision during datatransmission and help to reach each packet to the correct receiver without dropping. The wormhole attack is one of the most severe attacks in WANET which can significantly disrupt the communications across the network. Moreover, It is a type of replay attack and launched by one or more malicious node. The challenges of this attack is hard to defend against and easy to implement. This paper presents a novel approach for neighbor discovery and mitigating the effect of wormhole attack. The proposed system does not require any special hardware or expensive mechanisms added to the wireless nodes.

[7] In this paper, we develop an effective method called Wormhole Attack Prevention (WAP) without using specialized hardware. The WAP not only detects the fake route but also adopts preventive measures against action wormhole nodes from reappearing during the route discovery phase. Simulation results show that wormholes can be detected and isolated within the route discovery phase.

[8] In this paper, wormhole attack launched by exploiting AODV protocol in MANET, is detected and eliminated in two phases. The preliminary phase in the process of identifying wormhole attack is done, based on timing analysis and hop count. After suspecting the attack, a Clustering based approach is used to confirm the presence of attack, and also to identify the attacker nodes. The entire network is divided into different clusters and each cluster will have a Cluster Head, which controls all the nodes in the cluster and plays the role of a controlling authority in MANET.

[9] In this work, we introduce a novel approach for detecting wormhole attacks. The proposed algorithm is completely localized and works by looking for simple evidence that no attack is taking place, using only connectivity information as implied by the underlying communication graph, and total absence of coordination. Unlike many existing techniques, it does not use any specialized hardware, making it extremely useful for real-world scenarios. Most importantly, however, the algorithm can always prevent worm-holes, irrespective of the density of the network, while its efficiency is not affected even by frequent connectivity changes.

IV PROBLEM FORMULATION

The wormhole attack is a serious threat for mobile ad-hoc network. And it cannot be detected easily. For detection of the wormhole attack in MANET a technique has been proposed. In a wormhole attack, two attacker nodes join together. 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 [7]. The wormhole puts the attacker nodes in a very powerful position compared to other nodes in the network. In the reactive routing protocols such as AODV, the attackers can tunnel each route request packets to another attacker that is near to destination node. When the neighbors of the destination hear this RREQ, they will rebroadcast this RREQ and then discard all other received RREQs in the same route discovery process. This type of attack prevents other routes instead of the wormhole from being discovered, and thus creates a permanent Denial-of-Service attack by dropping all the data, or selectively discarding or modifying certain packets as needed.

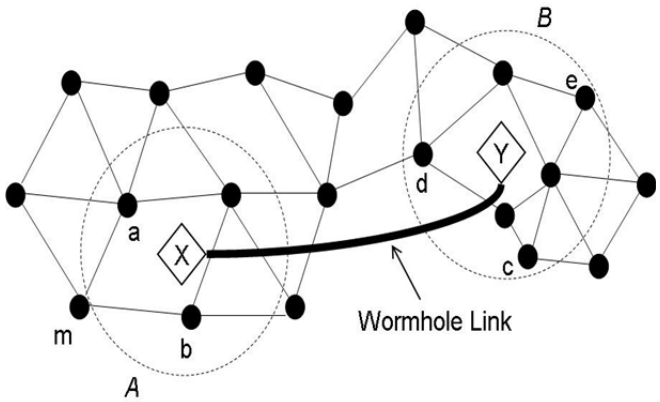

Figure 4: Wormhole Attack.

V CONCLUSION & FUTURE WORK

In this paper presents the review of wormhole attack detection and prevention technique. Also discuss the creation of wormhole attack in wireless network. The attack process is performed in terms of closed attack and open attack. The aim of wormhole attack is theft of information from source place. The attack of wormhole not much impact on the performance of wireless network. The performance of network basis is very difficult. In the process of detection process various algorithms is proposed by different algorithm such as reference based algorithm, clock synchronization and network packet coding technique.

REFERENCES

[1] ShiyuJi, 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] JuhiViswas, Ajay Gupta, Dayashankar Singh" WADP: A Wormhole Attack Detection Andprevention Technique in MANET using Modified AODV routing protocol" IEEE, 2013. Pp 376-381.

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

[5] BadranAwad, TawfiqBarhoom **"**BT-WAP: Wormhole Attack Prevention Modelin MANET Based on Hop-Count" IJARCCE, 2015. Pp 600-606.

[6] Rakhil R, Rani Koshy "An Efficient Algorithm for Neighbor Discovery and Wormhole Attack Detection in WANET"2015 International Conference on Control, Communication & Computing India (ICCC) 19-21 november 2015.

[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] AnjuJ,Sminesh C N,"An Improved Clustering-based Approach for Wormhole Attack Detection in MANET" 3rd International Conference on Eco-friendly Computing and Communication Systems 2014.

[9] TassosDimitriou and AthanassiosGiannetsos "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. Commun.Mob.Comput. 2006, Pp 483–503.