International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.01, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Wormhole Attack Detection in Wireless Network

Ratna Srivastava[1], Shalini Singh[2], Ms. Shweta[3]

Student[1], Student[2], Assistant Professor[3]

[1,2,3]Computer Science& Engineering, Buddha Institute of Technology Gida, Gorakhpur, (India)

ABSTRACT

Security and authentication of wireless communication is in current context. For the improvement of security and authentication use various method and techniques such as coding system, portal-based system, distributed algorithm and centralized algorithm in wireless network. These entire algorithms have certain limit in term of performance and network overhead. In this research paper, the algorithm for the detection of wormhole attack detection is discussed. The Wormhole detection is critical task in wireless network due to dynamic infrastructures and mobility of nodes. This survey paper presents a review of wormhole attack in mobile ADHOC network.

Keywords—Wireless Network, Wormhole Attack, Detection processes, Prevention processes, Attack Model.

I.INTRODUCTION

A collection of self-configuring mobile node without any communication network is called the Mobile adhoc network [4]. In a mobile adhoc network every node is connect via radio interface using wireless link so every node can free to move without any connection and without any rhyme with capability of variable link with other devices again and again [6].

Because of it is a multihope process, the partial communication range of energy constrained portable nodes and thus each tool in network topology as a router. Using dynamic nature of network topology, the routes changes very fast and a frequent and so the efficient routine protocols plays important rule in handling it. They should capable to ensure the delivery of packets safely on their destination.

Manets are also capable of handling topology changes and Malfunctions is nodes through network reconfiguration .Example, include on- the-fly conferencing application ,networking intelligent sensor devices etc.Interset in such dynamic wireless network is not new [1].They supported automatic route setup and maintenance in a packet radio network with adequate mobility .Interest in such networks has recently grown up due to the common availability of wireless communication devices that can connect Laptop and plamtops and operates in licence free radio frequency bands (such as the industrial scientific military are ISM band in the U.S).In an interest to run internetworking protocols on Adhoc network ,a new working group for mobile .Manet has been formed inside the internet engineering task force, whose chatters includes developing a framework for running internet based protocol in adhoc network .Interest has also been partly driven by the resent IEEE standard 802.11 that include the MAC and physical layer specification for wireless LANs without any fixed infrastructure [10].

Routing protocols in packets switched networks traditionally use either link state or distance vector routing algorithm. Both algorithm allow a host to find the next hope neighbour to reach the destination via the shortest path. The shortest path is usually in in term of the number of hops, however other suitable cost measures such as link utilization or queuing daily can also be used. Such shortest path protocols have been successfully used in many dynamic packets switched network. Distinguished example included use of link state protocol in open shortest path (OSPF) [9]. And used to distance vector protocol in roting information protocol for entirior routing in the internet. Even though, any such protocol would, in principle, work for adhoc network, a number of protocols has been usefully developed for used with adhoc networks. The primary motivation in that the shortest path protocol either link state or distance vector, take too long to converges and have a high message complexity. Because of the limited bandwidth of wireless links, messages complexity must be kept low. Also, potentially rapidly changing topology makes it important to find roots quickly even if the root may be suboptimal.

II. WORMHOLE ATTACK

In Wormhole attack two attacker nodes join together. One attacker nodes receive packets at one point and long underground passages them to another attacker node via a private network connection and then replays them into the network. Wormhole attack is a delay-based attack that can disturb the routing protocol [5] and therefore the network is breakdown and do to this reason this attack is very serious. We can explain about a general wormhole attack use four steps.

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 attackers then long underground passages the recorded attackers then long underground passages the recorded packets to different location. The attackers we terminate those packets back into the network location from simple wormhole in network.

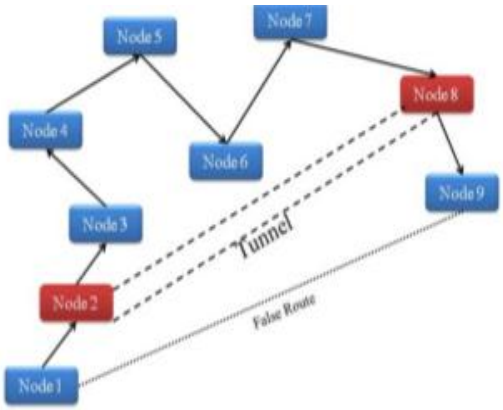

Figure:1: Example of Wormhole.

The simple wormhole in the network. Here node 2and node 8 create the tunnel in ordered to work as a malicious node. Both nodes give the illusion to another node that there is a smallest path. But this smallest path does not exist and attack can easily perform by the attacker. There are three types of Wormhole attack are available [9]. There are classified on the basis of its Nodes. There is 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: closed, half open, and open.

The examples that include nodes. 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 0from but not include". IN (a), M1.and M2. tunnel the neighbour discovery beacons from S to D and vice versa, for this reason S and D assume that they are direct neighbours to each other. M1 is a neighbour 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.

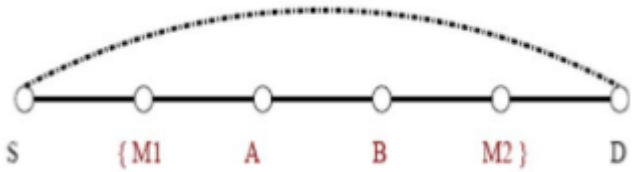

Figure 2: Closed wormhole attack

III. DETECTION AND PREVENTION PROCESSES

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

1. We justify wormhole vesting of harmful impact on network coding system performances through experiments. We proposed a centralized algorithm to detect wormholes and show its correctness regularize for the distributed wireless network, we proposed Dynamic adhoc wireless network (DAWN), a Distributed Detection Algorithm (DDA) against Wormhole in wireless Network coding system, by exploring the change of the flow direction of the innovative packets caused by wormhole. We strictly proved that dynamic adhoc wireless network guarantees a good lower bond of successful detection rate. We perform analysis on the resistance dynamic adhoc wireless network against collision attack.

2. Adaptive communication model is defined for wormhole infected mobile network. The presented model has provided the optimized parameter adaptive communication. Result shows that the work has improved the communication throughput and reduced the loss. This network for is defined is specification of relative problem

so that the protocol is also defined with specification of relative problem so that the adaptive communication is obtained from the work .the protocol defined with specification of the communication parameters ,architecture adaptive utilization and route formation .The first and mostly challenges 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. Some modification has been done in AODV routing protocol to detect and remove wormhole attack in real-world mobile adhoc network. Wormhole attack detection and prevention process algorithm, WADP, has been implemented in modified AODV. Also, node authentication has been used to detect malicious 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 kind of double verification for wormholes attack detection. Simulation result proves the theory

4. We present a countermeasure for the wormhole attack, called MOBIWORP, which alleviates these drawbacks and effecentiatelty mitigates the wormhole attacks in mobile network. MOBIWORP uses a source central authority (CA)for global tracking of more positions. Local monitoring is used to detect and isolate malicious nodes locally. Additionally, when sufficient suspicion builds up at the canter authority, its enforces a global isolation of the malicious nodes from the hole network. The effect of MOBIWORP on the data traffic and the fidelity of detection is brought out through extensive simulation using *ns-2*. The result show that as time progresses, the data packets graph 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 farming of a legitimate node by malicious nodes, at the cost of a slight increase in the drop ratio. The result also shows that increasing mobility of the nodes degrades the performance of MOBIWORP.

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

6. We proposed a new idea for neighbour's discovery process by introducing PR handshaking strategy. A PR handshaking strategy will analyse the activities of neighboring node and help to reduce collision during data transmission and help to reach packets to the correct receiver without dropping. The wormhole attack is one of the most sever attacks in WANET which can significantly throw into disorder the communications across the network. Moreover, it is a type of replay attack and launch by one or more malicious node. The challenges of this attack are hard to defend against and easy to implement. This paper presents a novel approach for neighbour's discovery and mitigating the effect of wormhole attack. The proposed system doesn't require any special hardware are expensive machines added to the wireless nodes.

7. 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 repairing during the route discovery phase.

8. 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 analyse and hope count. After suspecting the attack, a clustering-based approach is used to confirm the presence of attack, and also two identify the attackers' 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 rule of a controlling authority in MANET.

9. We introduced a Nobel approach for detecting wormhole attacks. The proposed algorithm is completely localized and Works by looking for simple evidence that no attacks is taking place, using only connectivity information implied by the underlying communication graph and total absence of co-ordination. Unlike many existing techniques it doesn't use any specialized hardware, making it extremely useful for real world scenarios. Most importantly, however the algorithm can always prevent worm-hole, irrespective of the density of the network while its efficiency is not affected even by frequent connectivity changes.

IV. ATTACK MODEL

A wormhole attack is composed of two attackers and a wormhole tunnel. To establish a wormhole attack, attackers create a direct link, referred to as a wormhole tunnel, between them. Wormhole tunnels can be established by means of wired link, a high-quality wireless out-of-band link, or a logical link via packet encapsulation. After building a wormhole tunnel, one attackers receive and copies packets from its neighbor's and forwards them to the other secret agreement attacker through the wormhole tunnel. This latter receives these tunneled packets and replays them into the network in its vicinity. In a wormhole attack using a wired link or a high-quality wireless out of band link, attackers are directly linked to each other, so they can communicate swiftly. However, they need special hardware to support such communication. A wormhole using packets encapsulation is relatively much slower, but it can be launched easily since it does not need any special hardware or special routing protocol.

V. CONCLUSION

In this paper, present the review of wormhole attack and detection and prevention techniques. The certain of wormhole attack in wireless network. The attack process is performed in term 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 algorithm is proposed by different algorithm such as reference-based algorithm, clock synchronization and network packet coding technique.

VI. ACKNOWLEDGEMENTS

Firstly, we would like to thanks Ms. Shweta (Asst.Professor) for him invaluable support, guidance and availability, throughout my survey paper, because without him support We couldn't achieved this success.
We would like to thanks all the participants for sparing the time to take part in this listen for my opinion. This acknowledgment would be incomplete if we could not express our respect to my parents and friends for their support.

REFERENCES

[1] ShiyuJi, Tingting Chen, Sheng Zhong *"Wormhole AttackDetection 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 forWorm Hole Preventive Route Optimization"* International Journal of Computer Science and Mobile Computing, 2015. Pp 80-85.

[3] Juridical, Ajay Gupta, Dayashankar Singh" *WADP: A Wormhole Attack Detection AND prevention 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 Model in 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 inWireless Networks"* 2012. Pp 1-14.

[10] J. Eriksson, S. V. Krishnamurthy, M Faloutsos*"True link: A practical countermeasure to the wormhole attack in wireless networks"* 2006, Pp 75–84.