A Review on Wormhole Detection and Prevention Technique

Megha Gupta¹, Prof. Rakesh Pandit²
Pursuing M.Tech¹, Assistant Professor 2
Patel Group Of Institutions, Indore 1,2
gmegha424@gmail.com , rakesh.pandit@patelcollege.com

ABSTRACT: - Wormhole attacks can undermine or put out of action wireless sensor networks. In a typical wormhole attack, the attacker be given packets at one point in the network, forwards through a wired or wireless network with take away latency than the network links, and transmits them to a different point in the network. This paper describes a give out wormhole recognition algorithm for wireless sensor networks, which detects wormholes based on the distortions they create in a network. Since wormhole attacks are passive in nature, a hop count technique is used by the algorithm as an explore procedure, renovates local maps in each node, and then uses a diameter element to detect abnormalities reason by wormholes. It can provide the approximate location of wormholes, which is useful in implementing countermeasures this is the main advantage of algorithms.

Keywords: wormhole detection, Wireless sensor network, distributed algorithm.

I. INTRODUCTION

Wireless sensor network (WSN) is talented technology consisting of small, low-power devices that integrate limited computation, sensing and radio communication capabilities. The technology has the potential to provide exile infrastructures for numerous applications, including healthcare, industry automation, observation and attack. Currently, most WSN applications are designed to work in trusted environments. However, security issues are a major concern when WSNs are deployed in entrusted environments. An adversary may put out of action a WSN by interfering with intra-network packet transmission via wormhole attacks, Sybil attacks, jamming or packet injection attacks. This paper focuses on wormhole attacks. In wormhole attack the malicious node receives packets at one point within the network, forwards them through a wired or wireless network with less latency than the network, and relays the packets to a different point in the network. Such an attack cryptographic knowledge; consequently, it puts the attacker in an influential position compared with other attacks (e.g., Sybil attacks and packet injection attacks), which make use of vulnerabilities in the network infrastructure. Indeed, a wormhole attack is possible even when the network infrastructure provides co veniality and authenticity, and the attacker does not have the cryptographic keys.

II. LITERATURE REVIEW

Raja Mohmood, R. A; Khan, A.I: According to these author the source node send two RREPs message, but selectively picking any consecutive RREP packets. This approach will likely appropriate in cases where a Wormhole node is located nearer to a source node and likely to underperform when it is located many hops away from the source node. A source node waits for a susceptible duration to receive other RREPs with next hop details from the other neighbouring nodes, without sending the DATA packets to the early RREP node. Simultaneous the expiry of the timer, it checks in CRRT table to find out any repeated next hop node. The chance of malicious path is limited if any repeated next hop node is present in the RREP paths. The simultaneous comparison of the received RREPs, selects a neighbour which has the equivalent next hop as other alternative routes to send the data packets. This solution adds a delay and decreases throughput as more RREPs are waited for, and the process of finding repeated next hop is an extra computation overhead.

Hao Yang, Haiyun Luo: They observe that how the AODV routing protocol works and then implemented Blackhole attack on it at the same time a trust based mechanism for its prevention. The trust based detection method has the better packet delivery ratio and correct Wormhole node detection probability, but suffered from the higher routing overhead due to the periodically broadcast packets. Another proposed mechanism i.e. reactive
detection method eliminates the routing overhead problem from the on demand way of route generation. Our complete implementation reveals that the proposed method of trust mechanism when applied on AODV protocol gives better results in all the cases for MANET as compared with normal AODV in case of Wormhole attack.

Xiao Yang Zhang; Sekiya; Y., Wakahara. Y.: Analyze the impact of the presence of the Wormhole nodes on the MANET performance. They found that as the percentage of Wormhole nodes increases, the network performance degrades.

Okoli Adaobi [04] et al worked to find the impact of Wormhole attack on the performance of MANET and also found the impact of position of Wormhole node. According to them under the on-demand routing protocol, the closer a malicious node is to the source of traffic, the greater extent of damage inflicted on the network.

N. Balaji, A Shanmugam,“A Trust Based Model to mitigate Wormhole attacks: In this paper we have presented a trust based routing model to deal with Wormhole and cooperative Wormhole attacks that are caused by malicious nodes. We believe that fellowship model is a requirement for the formation and efficient operation of ad hoc networks. The paper represents the first step of our research to analyse cooperative Blackhole attack over the proposed scheme to analyse its performance.

III. Wormhole Attacks

In wormhole attack the malicious node receives packets within the network, forwards them through a wired or wireless link with much less latency than the default network used by the network, and then relays them to an extra location in the network. In this paper, we assume that a wormhole is bidirectional with two endpoints, although multi-end wormholes are possible in assumption. A wormhole receives a message at its derivation end" and transmits it at its objective end." Note that the designation of wormhole ends as origin and destination are dependent on the context. We also assume that it does not send a message without receiving an inbound message and static i.e., it does not move.

IV. Wormhole Detection Algorithm

a hop counting technique as a probe procedure is used in our wormhole geographic distributed detection (WGDD) algorithm. After running the probe procedure, each network node collects the set of hop counts of its neighbour nodes that are within one/k hops from it. (The hop count is the minimum number of node-to-node transmissions to reach the node from a bootstrap node.) Next, the node runs Dijkstra's (or an equivalent) algorithm to obtain the shortest path for each pair of nodes, and reconstructs a local map using multidimensional scaling (MDS). Finally, a "diameter" feature is used to detect wormholes by identifying distortions in local maps. The procedure involved in the wormhole detection algorithm is described in the following sections.

V. Proposed Method:

The wormhole attack is presented in this paper in which two colluding nodes that are far away are connected by a tunnel giving an illusion that they are neighbours. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network from there. These nodes are able to advertise that they have the shortest path through them by using this additional tunnel. Once this link is established, the attackers may choose each other as multipoint relays (MPRs), which then lead to an exchange of some topology control (TC) messages and data packets through the wormhole tunnel. It results in spreading of incorrect topology information throughout the network [8] since these MPRs forward flawed topology information. On receiving this false information, other nodes may send their messages through them for fast delivery. It prevents honest intermediate nodes from source to the destination to establish links between them [11]. Sometimes, due to this, even a wormhole attacker may fall victim to its own success.

VI. Tools Required For Proposed Work

Themostreliableandauthenticatedtoolsusedandpreferredbymostoftheresearcherforthesekindsofsimulationsare:NS-2[23]and/orOPNETforreallookingsimulationsaccordingtotheirparameterprecisions.Inassociation,forvehicularmovementsonroads,anotherparticulartool ‘SUMO’
fortrafficmobilitypatternsgenerationisused. Accordi
ntoalreadymentionedresearchobjectives, themajore
mphasisofthisstudydependsontheanalysisof
MANETRoutingprotocols. These protocols need to be
compiled separately before associating with NS-
2simulation which would be receiving the TCL file(s) as
another input. The Tool Command Language (TCL) file
is scripting file for coding and developing the required
senarios – in this case vehicular flow on the road.

VII. CONCLUSION

This paper presents a hop count technique as a
search procedure for wormholes, reconstructs native maps using dimensional scaling
at every node, and uses a unique "diameter" feature
to find distortions made by wormholes. It
represents advancement over different wormhole detection
algorithms because it doesn't need anchor
nodes, further hardware (e.g., directional antennas
and correct clocks) or the manual setup of
networks. Even so, it will rapidly provide the
locations of wormholes that are beneficial for
implementing countermeasures because the
algorithmic rule is distributed, every node will potentially find the
distortions made by a wormhole that will
increase the chance of wormhole detection.

Simulation results demonstrate that the algorithmic
rule achieves an overall detection rate of close
to 100% (with an FTR near zero as shown in Figure
7(a)). Even just in case of shorter wormholes
that are less than 3 hops long, the algorithmic
rule has a detection rate of over 80% (with an FTR
of less than 20%). Moreover, the algorithmic
rule will be adjusted to provide extremely low false
alarm rates.

REFERENCES

and E. Cayirci, A survey of sensor networks,
102-114, 2002.
[2] S. Capkun, L. Buttyan and J. Hubaux,
SECTOR: Secure tracking of node
encounters in multi-hop wireless networks,
Proceedings of the First ACM Workshop on
Security of Ad Hoc and Sensor Networks,
[3] W. Du, L. Fang and P. Ning, LAD:
Localization anomaly detection for wireless
sensor networks, Journal of Parallel and
antennas to prevent wormhole attacks,
Proceedings of the Eleventh Network and
Distributed System Security Symposium,
detection in wireless ad hoc networks,
Technical Report TR01-384, Department of
Computer Science, Rice University,
Houston, Texas, 2002.
leashes: A defense against wormhole attacks
in wireless networks, Proceedings of the
Twenty-Second Annual Joint Conference of
the IEEE Computer and Communications
Bagrodia and B. Bhargava, Low-cost attacks
against packet delivery, localization and
time synchronization services in underwater
sensor networks, Proceedings of the Fourth
87-96, 2005.
[8] L. Lazos and R. Poovendran, SeRLoc:
Robust localization for wireless sensor networks,
ACM Transactions on Sensor Networks, vol. 1(1),
pp. 73-100, 2005.
location estimation in sensor networks,
Proceedings of the Fourth International
Symposium on Information Processing in
 simulator (ns-2) (nsnam.isi.edu
The sybil attack in sensor networks:
Analysis and defenses, Proceedings of the
Third International Symposium on
Information Processing in Sensor Networks,
routing for mobile ad hoc networks,
Proceedings of the SCS Communication
Networks and Distributed Systems
theoretic framework for preventing the
wormhole attack in wireless ad hoc
networks, Wireless Networks, vol. 13(1),
[14] The Rice Monarch Project, Wireless and
mobility extensions to ns-2
(www.monarch.cs.cmu.edu/cmu-ns.html),
2007.
J. da Mata, Survey on wireless sensor
network devices, Proceedings of the IEEE
Conference on Emerging Technologies and
Factory Automation, vol. 1, pp. 537-544,
2003.
[16] W. Wang and B. Bhargava, Visualization of
wormholes in sensor networks, Proceedings

