ISSN: 2394-7659
IMPACT FACTOR- 2.785

International Journal of Engineering Researches and Management Studies

MALICIOUS NODE AND WORMHOLE ATTACK DETECTIONS USING STATISTICAL TRAFFIC PATTERN ALGORITHM IN WIRELESS NETWORKS

S.Usha Devi*, A.Senthil Kumar
* Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010.
[2]Asst.professor, Dept.of.Computer science, Tamil University, Thanjavur-613010.

ABSTRACT

Network coding has been shown to be an effective approach to improve the wireless system performance. However, many security issues impede its wide deployment in practice. Besides the well-studied pollution attacks, there is another severe threat, that of wormhole attacks, which undermines the performance gain of network coding. In this paper, we quantify wormholes devastating harmful impact on networks coding system performance through experiments. We first propose a centralized algorithm to detect wormholes and show its correctness rigorously. We propose STPA, Statistical Traffic Pattern 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 Statistical Traffic Pattern Algorithm (STPA) guarantees a good lower bound of successful detection rate. We perform analysis on the resistance of Statistical Traffic Pattern Algorithm (STPA) against wormhole attacks. We find that the robustness depends on the node density in the network, and prove a necessary condition to achieve wormhole resistance

Keywords:- *Nodes, Authentication, Data Transfer, Traffic Capture..*

I. INTRODUCTION

Mobile Computing is a human-computer interaction by which a computer is expected to be transported during normal stage. Mobile computing involves mobile communication, mobile hardware, and mobile software. This project briefs that to provide high anonymity protection for sources, destination and route with implementing the low cost and the reliable architecture called MANET known as Anonymous routing protocol [1]. Statistical Traffic Pattern Algorithm (STPA) it aims to derive the source and destination probability distribution, i.e., the probability for each node to be a message source and destination, and the end-to-end link probability distribution[3]. The Probability for each pair of nodes to be an end-to-end communication pair.

II. EXISTING SYSTEM

The connectivity in the network is described using the link loss probability value between each pair of nodes, while traditional networks use connectivity graphs with a binary relation (i.e., connected or not) on the set of nodes. Some other existing works rely on the packet round trip time difference introduced by wormhole attacks to detect them [2]. Unfortunately, this type of solutions cannot work with network coding either. They require either to use an established route that does not exist with network coding, or to calculate the delay between every two neighbouring nodes which will introduce a huge amount of error in network coding systems

Existing System Disadvantages

- A point-to-point message transmission usually has only one possible receiver.
- MANETs lack in security and performance.

III. PROPOSED SYSTEM

We first propose a centralized algorithm to detect wormholes leveraging a central node in the network. For the distributed scenarios, detect wormhole attacks in wireless intra-flow network coding systems [5]. For bothCentralized and distributed algorithms, we have utilized the digital signatures to ensure every report is undeniable and cannot be forged by any attackers.

ISSN: 2394-7659
IMPACT FACTOR- 2.785

IJERMS

International Journal of Engineering Researches and Management Studies

Advantage Of Proposed System

In our approach a novel **Statistical Traffic Pattern Algorithm (STPA).** STPA aims to derive the source and destination probability distribution, the probability for each node to be a message source and destination, and the end-to-end link probability distribution, the probability for each pair of nodes to be an end-to-end communication pair[4]. STPA include two major steps:

1) Construct point-to-point traffic matrices using the time-slicing technique, and then derive the end-to-end traffic matrix with a set of traffic filtering rules.
2) Apply a heuristic approach to identify the actual source and destination nodes, and then correlate the source nodes with their corresponding destinations.

- It captures the raw traffic from the PHY/MAC layer on end-to-end.
- It provides security and performance high.

IV. PROCEDURE

Authentication
Input: User identities such as Username, Password.
Output: Granting Access privilege
Sender
Input: Capturing traffic on nodes, source node, destination node, upload data and send file**.**
Output: Send to Sub nodes.
Intermediate Nodes
Input: Collect data from source node.
Output: Send to destination through Sub node.
Receiver
Input: Collect data from Sub node.
Output: Store in Data base.
Attacker
Input: Monitor data transfer on sub nodes.
Output: Discover traffic pattern.

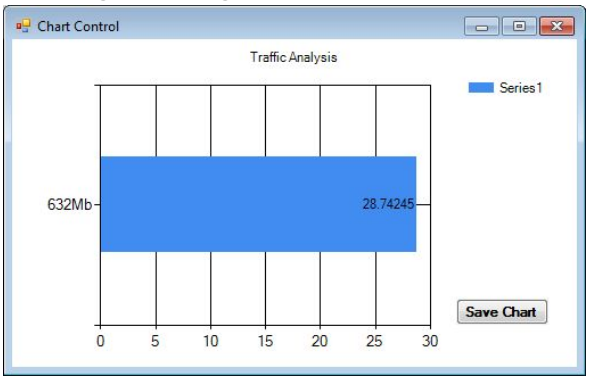
V. PERFORMANCE ANALYSIS

The necessary and sufficient conditions for any transformation to remove wormholes, and showed that any candidate solution preventing a wormhole attack must produce a connected sub graph of the geometric graph model of the network. A cryptography-based solution relying on local broadcast keys and provided a distributed mechanism for establishing them in randomly deployed networks. Analytically determined the level of security achieved by our scheme based on spatial statistics theory. The appropriate choice of network parameters eliminates wormhole links with a probability close to unity and verified the validity of our results via simulations. It is our claim that in the absence of location or distance bounding, we must use probabilistic techniques for dealing with wormholes. A solution that treats Wormhole attack problem by using cryptographic approach i.e. RSA and Multipath Routing concept. Our proposal will improve data security robustly .This approach in wireless Ad hoc Networks, increasing the transmission speed in security environment. Because, dividing the initial message and exploiting the characteristic of existence of multiple paths between nodes in an Ad hoc network and also increase the robustness of confidentiality. The metrics used in this research are each pair modes transmission, packet range, hidden traffic pattern are utilized.

ISSN: 2394-7659
IMPACT FACTOR- 2.785

IJERMS

International Journal of Engineering Researches and Management Studies



In the above pitcure, analysis process approximately 632Mb of data can send only within the traffic limit of maximum 30 otherwise the data may be lost (or) hacked by some other attacker.

VI. CONCLUSION

A novel statistical traffic pattern Algorithm (STPA). It performs to derive the source/destination probability distribution, i.e., the probability for each node to be a message source/destination, and the end-to-end link probability distribution. The probability for each pair of nodes to be an end-to-end communication pair. In STPA, the actual receiver of a point-to-point transmission is not identifiable among all the potential receivers within the sender's transmitting range. This inaccuracy can be mitigated in GSTARS because most potential receivers of a packet will be contained within one or a few super nodes. GSTARS will be the direction of our future research. In this future improvement of the traffic analysis corresponding to the heuristic data processing model to reveal the hidden traffic patterns from the end-to-end matrix. Then intimate to sender's part based on hidden traffic nodes capturing. For its distributed scenarios, the proposed work uses statistical traffic pattern in a robust way and emphasizes node density and information security and has proved a necessary method to reduce intrusion occurrence. In its analysis, it organizes the nodes as both sender and receiver and the intermediate node placement to detect the wormhole attack and proves the normal attack detections confident ably (i.e.,) 60% level of detection accuracy to achieve information security.

VII. FUTURE ENHANCEMENT

A wormhole tunnel can actually be useful if used for forwarding all the packets, it puts the attacker in powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network. In wormhole attack the two remote regions are directly connected through nodes (malicious) that appear to be neighbors but are actually distant from one another. Such wormhole attack results in the false route. So the wormhole attack is one of the most severe threats to ad-hoc networks, as it can do harm to both sender and receiver by performing packet dropping or alteration. This research suggests on countermeasures that analyses traffic pattern in network provides alternate path suggestion to reduce wormhole attack threats. In future, the traffic pattern can be measured equivalently with respect to time or nonce proposal to detect wormhole attacks compromising nodes. Recent simulation tools apart from daily software can be used to analyse wormhole attack detections there by, enriching information security principles.

ISSN: 2394-7659
IMPACT FACTOR- 2.785

International Journal of Engineering Researches and Management Studies

REFERENCE

1) *ShiyujiTingting Chen, Sheng Zhong Oklahoma State University, {Shiyu, tingtic}@cs.okstate.eduNanjingUniversity,zhonogsheng@nji.edu.cn.*
2) *S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks," Proc. IEEE 20th Int'l Conf. Advanced Information Networking and Applications Workshops (AINA Workshops '06), pp. 133-137, 2006.*
3) *J. Kong, X. Hong, and M. Gerla, "An Identity-Free and On- Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 6, no. 8, pp. 888-902, Aug. 2007.*
4) *DhirenR.Patel,"informationsecurity", http://www.phindia.com.*
5) *"Priniciple and practices of information security", Michael E.whiteman, Herbert J ,Mattord,CENGAGE Learning , India Edition, 2009.*