International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4
ISSN: 2454-4248
770 – 773

An Improved Wormhole Attack Detection and Prevention Method for Wireless Mesh Networks

Thumpala Vasantha Lakshmi
Computer Science And Engineering
Guru Ghasidas University
Bilaspur,India
vasantha8440.vv@gmail.com

Nishi Yadav
Assistant professor
Guru ghasidas university
Bilaspur, Chattisgarh
Mail id- nishidv@gmail.com

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. Since the underlying characteristics of network coding systems are distinctly different from traditional wireless networks, the impact of wormhole attacks and countermeasures are generally unknown. 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 and the efficiency of DAWN.

Keywords: *WMN; Attacks;Security; Routing.*

*****

I. INTRODUCTION

In the range of discussion the customary worried systems are destroy because of the remote age. The remote innovation is ease, low upkeep, and quick installable. In this manner various indoor and out of entryways group innovation are progressed to serve steady with the need of administrations. Among some of particular advances the remote work arrange is one of the imperative innovations. The remote work systems (WMNs) are exceptionally valuable in view of its self-reclamation and self-arranging nature. That can be utilized for versatile portable systems, organization systems, group systems; and so on. The WMN is a total switches and clients, where switches set up a remote availability to the customers. WMN have various advantages which incorporate lowsetup cost, enhanced scope and furthermore displays bendy and trustworthy administrations . Because of its portable and remote nature the ordinary discussion can be hindered by utilizing the pernicious assailants which incorporates Wormhole, Black-empty, Gray-opening and others. These assaults not just influence the offerings of the group it additionally influence the system general execution of system radically.

II. WORMHOLE ATTACK

Wormhole assault is a particular type of inner assault, wherein malevolent nodes within the network plan to establish an imaginary channel between them. This channel can be an out-of-band excessive-speed verbal exchange hyperlink or can hire in-band tunnelling approach to bypass intermediate nodes. This wormhole hyperlink is typically mounted between two colluding nodes located a long way away inside the network. Once diagnosed, the wormhole captures a variety of site visitors because it advertises a whole lot higher hyperlink metric than some other paths in the network. The wormhole nodes can then initiate diverse sorts of denial of carrier (DoS) assaults that strictly affect the habitual of the network. It is very tough to locate this form of assault as the nodes worried within the network action form genuine part of the network and simply cryptographic mechanisms can't prevent such kind of assault.

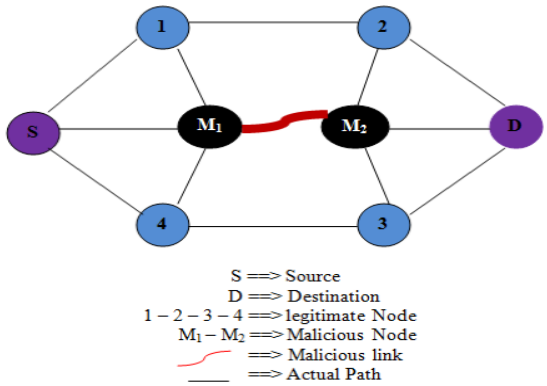


Figure 1 Wormhole Attack

III. PROPOSED ARCHITECTURE

In this section, the idea to detect wormhole attack is presented based on the knowledge gathered on the survey. In the review papers various techniques have been adopted to detect the wormhole attack. In my proposed work there is a centralized and distributed algorithm to detect wormhole. Here we define a threshold value for data transfer. We

 ISSN: 2454-4248
406 – 411

consider a public key infrastructure for implementing the public key infrastructure. In wireless network we consider each node as a user that has a pair of private and public keys. There is a central authority (CA) in the infrastructure which maintains the identity information of each user. It is a trusted entity which is also responsible for pre-distributing and revoking the key. During the data transfer the sender will request the receiver public key for encrypting the data and the receiver will request the sender public key from CA for decrypting the data. Here when the data transfer takes place the centralized node will monitor whether any innovative packets arrives to a node within the communication range. Each node has a rank and time stamp value. If innovative packets arrive then the rank of each node will be incremented. Next the centralized algorithm will calculate the expected transmission count (ETX) that describes the expected total number of transmission to complete the data transfer. If the ETX value exceeds the threshold value then the centralized algorithm will find the wormhole links. In case if there is no central node to monitor the nodes, then the distributed algorithm takes place. Here the entire network is divided into the cluster. The cluster head will be chosen from each cluster and then assign the role to monitor the nodes. The distributed algorithm will takes place in absence of centralized node. Thus the centralized and distributed algorithm provides a greater contribution in detecting the wormhole attack. The overall architecture is presented below, where the centralized algorithm technique is implemented to detect the wormhole attack.

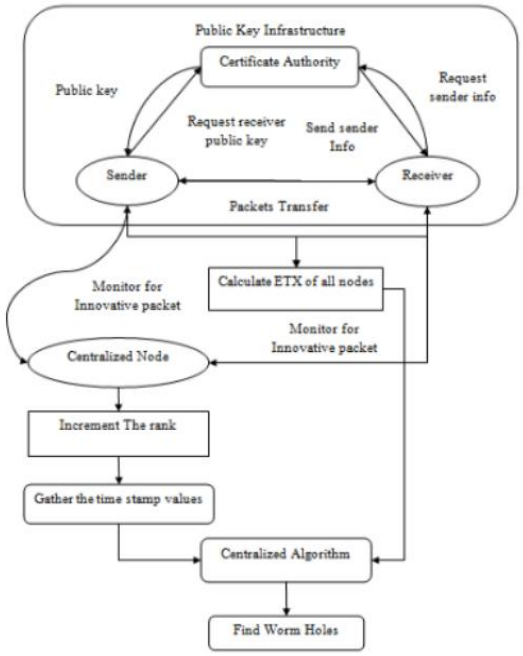


Fig 1. Architecture

IV. IMPLEMENTATION

Algorithm to Determine ETX

Input: the entire network G with nodes V and their locations L, and the source node v_s
Output: the ETXs for all the nodes in the network G

$ETX(v_s) \leftarrow 1.0$
for each node v_i in V, except v_s **do**
  $ETX(v_i) \leftarrow +\infty$
end for
repeat
  $ETX_{updated} \leftarrow$ false
  for each node v_i in the network G, other than v_s **do**
    Let N be the set of the neighbors of v_i s.t. $ETX(v_k) < +\infty$ for any $v_k \in N$
    if $ETX(v_i) > \frac{1}{1-\prod_{v_k \in N} \frac{1}{ETX(v_k)}(1-P(v_k,v_i))}$ **then**
      $ETX(v_i) \leftarrow \frac{1}{1-\prod_{v_k \in N} \frac{1}{ETX(v_k)}(1-P(v_k,v_i))}$
      $ETX_{updated} \leftarrow$ true
    end if
  end for
until $ETX_{updated}$ = false
return the ETXs for all the nodes

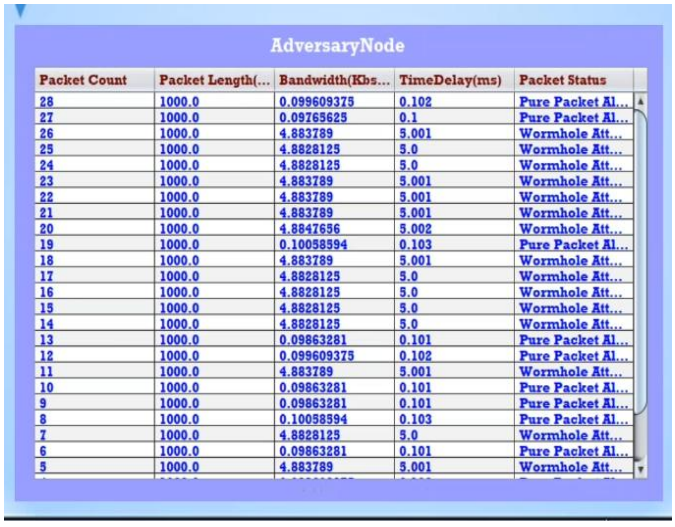
The Centralised Algorithm

In this section, we propose the centralized algorithm, which utilizes the ETX metric and the order of rank increment to detect wormhole attacks. In order to protect the validity of our method, we also introduce the public cryptographic scheme for the network. For the proposed algorithm, we not only perform the analysis of its correctness, but also discuss its technical details in this section.

Simulation Scenario

In order to perform the experiments the following one-of-a-kind scenarios are prepared for simulation and community overall performance opinions.

1. Simulation underneath AODV Routing Protocol with Wormhole Attack: on this community simulation the network is configured with AODV routing protocol and the network performance is evaluated. That simulation additionally incorporates a malicious wormhole hyperlink which demonstrates the results of wormhole attack in ordinary community.


AdversaryNode

Packet Count	Packet Length(...	Bandwidth(Kbs...	TimeDelay(ms)	Packet Status
28	1000.0	0.099609375	0.102	Pure Packet Al...
27	1000.0	0.09765625	0.1	Pure Packet Al...
26	1000.0	4.883789	5.001	Wormhole Att...
25	1000.0	4.8828125	5.0	Wormhole Att...
24	1000.0	4.8828125	5.0	Wormhole Att...
23	1000.0	4.883789	5.001	Wormhole Att...
22	1000.0	4.883789	5.001	Wormhole Att...
21	1000.0	4.883789	5.001	Wormhole Att...
20	1000.0	4.8847656	5.002	Wormhole Att...
19	1000.0	0.10058594	0.103	Pure Packet Al...
18	1000.0	4.883789	5.001	Wormhole Att...
17	1000.0	4.8828125	5.0	Wormhole Att...
16	1000.0	4.8828125	5.0	Wormhole Att...
15	1000.0	4.8828125	5.0	Wormhole Att...
14	1000.0	4.8828125	5.0	Wormhole Att...
13	1000.0	0.09863281	0.101	Pure Packet Al...
12	1000.0	0.099609375	0.102	Pure Packet Al...
11	1000.0	4.883789	5.001	Wormhole Att...
10	1000.0	0.09863281	0.101	Pure Packet Al...
9	1000.0	0.09863281	0.101	Pure Packet Al...
8	1000.0	0.10058594	0.103	Pure Packet Al...
7	1000.0	4.8828125	5.0	Wormhole Att...
6	1000.0	0.09863281	0.101	Pure Packet Al...
5	1000.0	4.883789	5.001	Wormhole Att...

Figure 2 Networks under Attack

 ISSN: 2454-4248
406 – 411

2. Simulation for Proposed Method under AODV Routing Protocol with Attack Prevention: n this simulation the proposed comfortable routing protocol is applied in the community simulator 2 with the same configuration as the alternative networks is configured. After that for investigating the impact of the proposed answer the wormhole link is applied on the community and the network performance is predicted via end result evaluation.

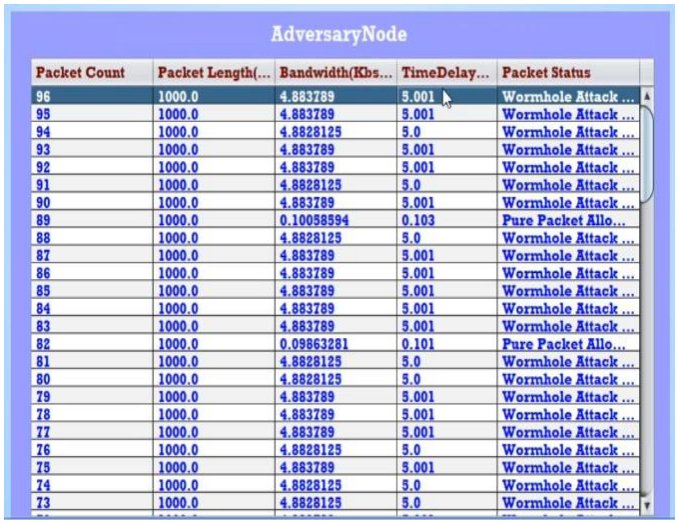


Figure 3 Proposed Method

5. RESULTS ANALYSIS

Graphs are plotted and concluded that proposed scheme has improve throughput value and packet shipping ratio also reduces end to stop routing put off.

1. End to quit put off

End to give up delay on network refers to the time taken for a packet to be transmitted throughout a network from supply to vacation spot tool.

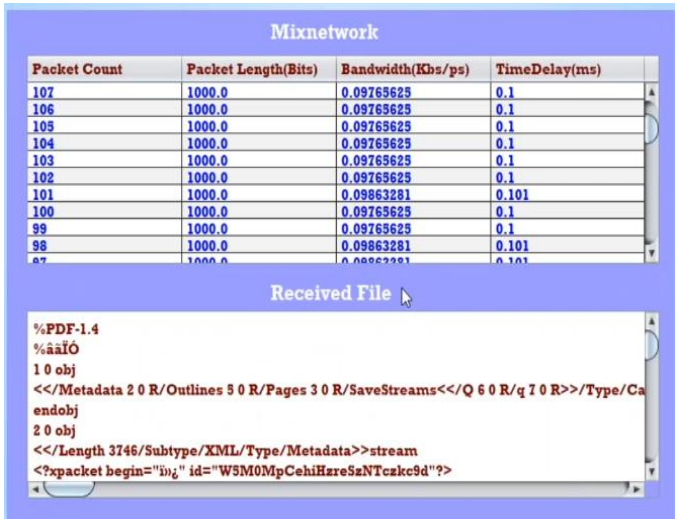


Figure four End-to-End Delays

cease to quit delay in phrases of milliseconds. The overall performance of the proposed approach is simulated thru inexperienced line.

2. Packet Delivery Ratio

Packet transport ratio gives facts about the performance of any routing protocols, where PDR is expected the usage of the system given Packet Delivery Ratio = Total Received PacketsTotal Sent Packets In this diagram the X-axis indicates the simulation time of the community and the Y-axis indicates the packet shipping ratio in phrases of percent.

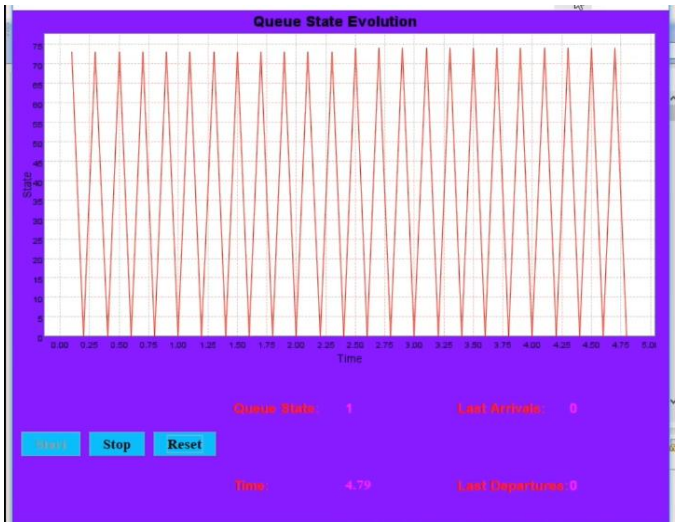


Figure five Packet Delivery Ratio

6. CONCLUSION AND FUTURE WORK

Remote work systems are at risk to extensive variety of insurance assaults because of their arrangement in an open and unprotected environment. This examinations work explores special wormhole recognition methodologies, looks at different existing techniques to find how they were done to unearth wormhole ambushes. Every method has its own special quality and shortcomings. We offered a proficient system to spare you Wormholes on WMN. The proposed instrument is shortsighted and does now not depend on additional like GPS frameworks. The execution of the proposed strategy is given the utilization of the java environment. For general execution examination is executed utilizing the produced arrange follows. The general execution of the actualized steering approach is imagined as far as parcel conveyance proportion, throughput, and quit to end delay.

V. Future Work

The proposed approach can be reached out by the utilization of various situations in systems.

1. The given strategy is a parameter essentially based method which uses the system parameters for finding the vindictive connection subsequently that approach can be drawn out for actualizing security for various assaults basically in view of the system parameter choice.
2. The Future Scheme of the whole research is to expand the proposed plan to various conventions instead of the AODV convention. The system is intense and productive at some phase in strike conditions subsequently the method is

 ISSN: 2454-4248
406 – 411

utilized for likewise to improve thesystem security in different remote advert hoc systems comprehensive of VANET, WSN and others.

REFERENCES

[1] IAN F. AKYILDIZ, XUDONG WANG, "A Survey on Wireless Mesh Networks", IEEE Radio Communications, September 2005, 0163-6804/05/$20.00 © 2005 IEEE

[2] S. A. Ade and P. A. Tijare, "Execution Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 545-548, July-December 2010

[3] Nikhil Kumar, Vishant Kumar and Nitin Kumar, "Close Study of Reactive Routing Protocols AODV and DSR for Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies (IJCSIT), Volume five, pp.6888-6891, 2014.

[4] M. S. Karthikeyan, K. Angayarkanni, and Dr. S. Sujatha, "Throughput Enhancement in Scalable MANETs the use of Proactive and Reactive Routing Protocols", In Proceedings of the International Multi Conference of building and programming designing, Volume 2, March 2010.

[5] Hu, Y. Perrig, An., and Johnson D., Packet Leashes: "A Defense against Wormhole Attacks in Wireless Network", In Proceedings of the twenty second IEEE International Conference Computer and Communications, Volume three, pp.1976– 1986, April 2003.

[6] P. V. Tran, L. X. Hung, Y. Lee, S. Lee, and H. Lee, TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-Hoc Networks, In Proceeding of fourth IEEE CCNC, pp. 593-598, Las Vegas, USA, Jan. 2007.

[7] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," In Network and Distributed System Security Symposium (NDSS), San Diego California, USA, five-6 February, 2004.

[8] S. Capkun, L. Buttyan and J.P., Hubaux, "Part: Secure Tracking of Node Encounters in Multi-hop Wireless Networks", In Proceedings of first ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS), pp. 21-32, New York, USA, 2003.

[9] L. Lazos and R. Poovendran, "Serloc: Secure collection fair control for Wireless Sensor Networks", In Proceedings of the ACM Workshop on Wireless Security, pp. 21−30, October 2004.

[10] P Subhash and S Ramachandram, "Maintaining a strategic distance from Wormholes in Multihop Wireless Mesh Networks", Third International Conference on Advanced Computing and Communication Technologies, pp. 293-three hundred, 2013.

[11] H.S. Chiu and K.S. Lui, "DELPHI: Wormhole Discovery Device for Ad-hoc Wireless Network", first International Symposium on Wireless Pervasive Computing, pp. 6– 11, Phuket, Thailand, sixteen-18 January 2006.

[12] C. Sun, K. Doo-more young, L. Do-hyeon and J. Jae-il, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," In Proceeding of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), pp. 343-348, 2008.

[13] I. Khalil S. Bagchi and N.B. Shroff. LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multi-skip Wireless Networks, International Conference on Dependable Systems and Networks, pp.612– 621, 2005.

[14] W. Wang and B. Bhargava, "Portrayal of wormholes in sensor frameworks", In Proceedings of the third ACM workshop on Wireless security, October 01, Philadelphia, PA, USA, 2004.

[15] The Network Simulator. NS-2 [Online] http://www.Isi.Edu/nsnam/ns