Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 8, August 2015, pg.80 – 85

RESEARCH ARTICLE

A Parameter Estimation Based Model for Worm Hole Preventive Route Optimization

Amit Kumar

Student, M.Tech, Dept. Of Computer Sc. & App., Pratap university, Jaipur

E.mail: bishnoi17amit@gmail.com

Sayar Singh Shekhawat

Associate Professor, Dept. Of Computer Sc. & App., Pratap University, Jaipur

E.mail: sayarss@rediffmail.com

Abstract— Security is most critical issue aspects for mobile network. A network in public domain suffers from various internal and external attacks. Worm Hole is one of such attack in which two or more nodes collectively access the bandwidth and disturb the communication. In this present work, communication parameter based analysis model is presented to provide the safe communication under worm hole attack. The results obtained from work shows that the work has improved the communication and reduced the communication loss.

Keywords— MANET, Security, Wormhole, Parameter Based

I. INTRODUCTION

Mobile network is the network defined in public domain which provides the long distance cooperative communication. It is the most common form of adhoc network in which the communication without the specification of any infrastructure. 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. The speed in these networks is generally not directed. It means node can randomly move in any direction so that the analysis over the network can be performed based on different parameter. This kind of parameter based analysis can be applied to provide the safe communication in the network. This network form provides the safe communication. The dynamic nature of this network and the frequent change is architectural or the node position increase the communication criticality. The network also allows the inclusion and exclusion of nodes in the network. This movement based dynamic nature also switch between different coverage areas so that the switching to the base station also a

criticality of the network model This kind of vehicle switch increases the network deficiencies and the network criticality is also increased. These all issues to the network are based on the communication aspect. Another critical issue in mobile network is the security.

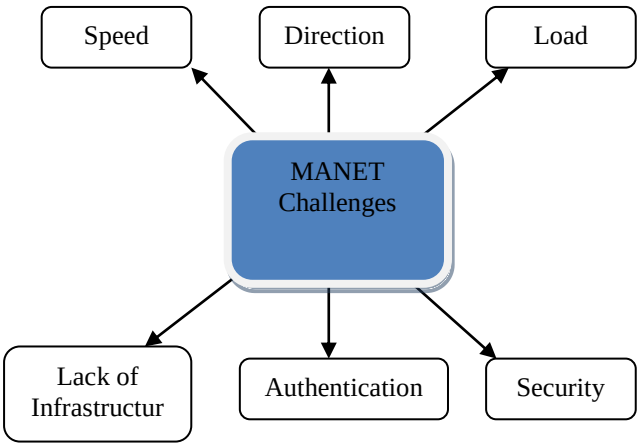

Figure 1 : MANET Issues

The security in a public network is considered as the most critical communication issue. The security threats affects the network at different levels and in different layers. These security threats can be generated by internal as well as external network nodes. The security threats can be node specific, application specification or the communication specific. There are number of associated issues collected to provide the reliable communication to optimize the communication. These network solutions include the authentication adaptive security, preventive security and the attack specific security. The authentication is some kind of verification of a node under reliability vector. A node which is more stable and reliable is considered as adaptive for mobile communication. Another method for reliable communication and the communication aspect based optimization can be achieved using preventive approach. To provide the safe communication over the network, the preventive communication can be performed over the network. The final work associated with this research is the attack specific security. Network suffers from various internal and external attacks. These attacks affect the network in different ways. The attack constraint specific model can be applied to identify the attacked nodes and block the communication over these nodes. In this paper, one of such attack affected problem can be resolved. In this paper, the work is defined for wormhole attack detection and providing the safe communication over the network.

A) Wormhole Attack

Worm attack is the crucial attack applied by internal network nodes cooperatively. These nodes form a tunnel and provide a loop based communication over the tunnel. As any of the node occurs in a communication path, it avoid the delivery to the destination end. This kind of communication disturbs the network communication and increases the communication delay. This attack form avoids the packet forwarding so that the overall communication throughput is decrease and the communication loss increases.

In this paper, a safe communication model is presented against the wormhole attack. The presented work model is defined against the wormhole attack. In this section, an exploration on MANET issues is defined. The section also identified the security issues and specially wormhole attack. In section II, the work defined by earlier researchers is discussed. In section III, the presented research work is defined. In section IV, the results obtained from work are presented. In section V, the conclusion of the work is defined.

II. EXISTING WORK

In this section the work defined by earlier research is discussed and presented. Capkum[1] has presented a sector adaptive node synchronization model for attack detection. Author analyzed the distance bounding based analysis with authentication measure for estimation of the reliable communicating node. Author defined the time bound adaptive analysis applied to analyze the cooperative neighbor. Once the neighbor is identified, the attack specific modeling is applied for attack detection in the network. Leash[2] also presented a study on the wormhole attack and its defensive measures. Author defined the packet design based transmission control mechanism under distance analysis. Author presented two main model for analysis called temporal and geographical model. The temporal model where analyzed the time bound synchronization

over the communication and the geographic model analyzed the communication under positional aspects. The position and transition based analysis has provided the safe and adaptive communication in network. Author[3] defined directional antenna based modeling for optimizing the communication under cluster adaptive analysis. Author provided the message communication for wormhole discovery and provided the exclusive communication mechanism in the network. Author presented the trust adaptive communication route generation model to optimize the network communication. Chiu[4[proposed a hop analysis model identification of the load and delay on each communicating neighbor. Author defined the propagation analysis based hop adaptive path diversity modeling so that the adaptive communication mechanism will be formed over the network. This network model is defined for optimizing the network communication and provided the secure communication over the network.

Author[5] defined the wormhole attack in reference to the mobile network protocols and conclude the illusion in the remote regions so that the throughput adaptive neighbor node communication will be formed. Author provided the directly connected network model for optimizing the communication and provided the communication in attack network. Author optimized the network security under speed off link. Author[6] Also identify the channel band observation to optimize the network communication under delay analysis. Author defined a tunnel preventive model to optimize the communication and to generate the safer and shorter path. Author also minimizes the visit over any of the tunnel node based on the memory adaptive recording. Author[7] has defined a route formation based model to analyze the communication hop count so that the reliable communication route will be formed over the network. This network model assigned the priority to the routing nodes and provided the solution under eavesdropping, packet modification and DOS attack. Author provided the routing solution against wormhole attack.

Author[8] generated a hop driven communication analysis model for effective communication formation in the mobile network. Author provided the wormhole detection under two step analysis. This analysis is provided on the path length and provides the analysis on advertised path. Author defined the route information collection model so that the timestamp based communication will be formed. The consecutive formation and threshold specific communication will be formed. Gorlatva[9] defined a work on the wormhole attack identification technique for attack identification. Author defined the time interval based control message generation for optimized link identification. The range specific analysis is here applied for optimizing the network communication in the network. Shalini[10] also proposed the trustable scheme for isolating node analysis for wormhole attack identification. Author defined the cryptographic model for malicious node identification and colluding node specification in the network. the operational activity is observed to generate the path. Author[11] defined an optimization to the AODV protocol against the wormhole attack and provided the communication solution under evaluation test. Author defined the statistical measure based model for route optimization and route generation under the aspect derivation. This model has analyzed the Request time for the optimization of communication over the network.

III. PROPOSED MODEL

Mobile network is the critical network form defined in public area. This network model suffers from different internal and external attacks. In this paper, a wormhole infected network is defined and the work model is provided to perform the reliable communication in attacked network. The work is here defined to generate the network model for optimizing the communication to identify the safe communication node.

In a mobile network, the nodes are present in the form of high speed moving nodes. When nodes communicated with cooperatively to perform the communication. If some wormhole attack is present on these intermediate nodes, then the attack adaptive analysis is performed over the node. This analysis is here performed under different communication vectors. In first layer, the distance adaptive analysis is applied to obtain the neighbor nodes. The cooperative communication is performed to provide the safe communication in the network. In second layer, the communication analysis is performed. The communication parameters includes packet loss analysis and communication delay analysis. Based on these parameters the identification of adaptive neighbor node is done. This stage has identified the wormhole based on the attack specific measures. The work also identified, the safe communication node based on which the communication can be applied to deliver the information.

In this network model adaptive network analysis is performed to generate the effective communication analysis and relatively safe communication path is obtained from the work. The work is here defined to generate the safe path in attack based mobile network.

In this network model association based approach has been implemented to identify the safe node to perform the communication

- If the response time of a node is less than the Threshold AND
- Throughput of the node is greater than Throughput Threshold AND
- Delay should be less then Delay threshold.

If all these three conditions are satisfied, the current node will be considered as an eligible node for communication and it performs communication to next node in the network otherwise this node is considered to be an unreliable node of the network.

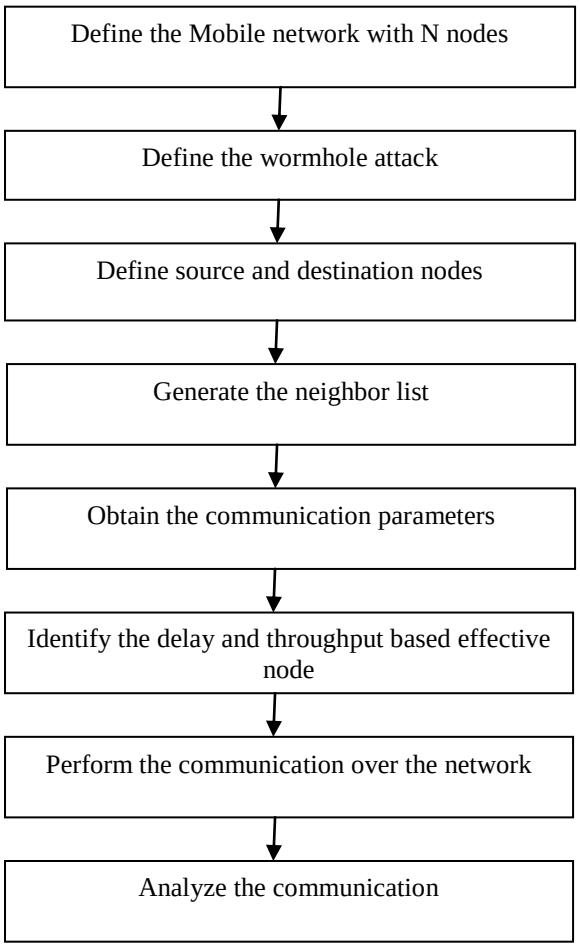

Figure 2 : Flow of Work

IV. RESULTS

In this present work, parameter adaptive communication model is presented for safe communication in wormhole infected network. The work is here defined based on the communication parameters. In first level the neighbor node analysis is done and later on the communication analysis based safe path is obtained. The work is implemented in NS2 network. The simulation parameters considered in this work are shown in figure 1

Table 1 : Simulation Parameters

Parameter	**Value**
Number of Nodes	26
Position	Random
Type of Node	Mobile
Simulation Time	100sec
Network Area	100x 100

Data Rate	10.2e6
Bandwidth	20.0e6
Propagation model	Two ray ground
Antenna Model	Omni directional
MS Speed	Random

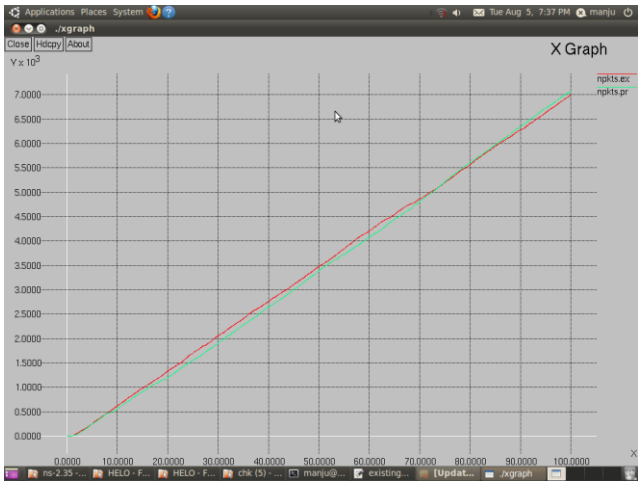

Figure 3 : Packet Communication Analysis

Figure 3 is showing the comparative analysis of this work in terms of packet communication. The figure shows that the presented work model has improved the network communication and network throughput. The work has improved the network effectiveness and provided the reliable communication over the network.

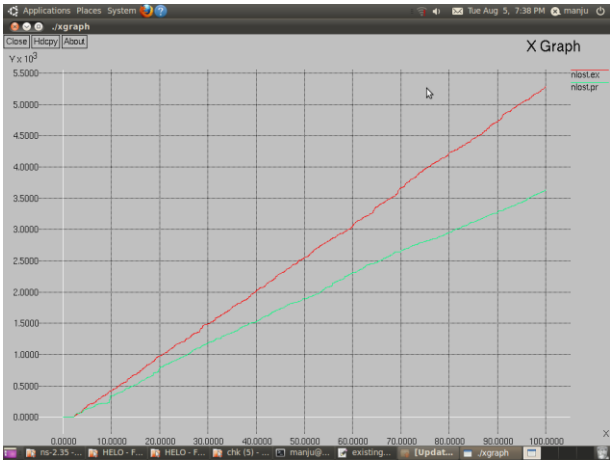

Figure 4 : Communication Loss Analysis

Figure 4 is showing the comparative analysis of this work in terms of packet loss. The figure shows that the presented work model has reduced the network loss so that the reliability of the work is improved

V. CONCLUSION

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.

REFERENCES

[1] 1. Srdjan Capkun, L.evente Buttyan, and Jean-Pierre Hubaux, 2003 "SECTOR: Secure Traking of Node Encouters in Multi-hop Wireless Networks,"In Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS), pp. 21-32.

[2] 2. Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 "Packet Leashes : A Defence against Wormhole Attacks in Wireless Networks", Twenty-Second ANNUAL Joint Conference of IEEE Computer and Communications , pp. 267-279.

[3] 3. Lingxuan Hu and David Evans, Feb. 2004 "Using Directional Antennas to Prevent Wormhole Attack ",In Proceedings of the Network and Distributed System Security Symposium, pp. 131-141.

[4] 4. Chiu, HS; Wong Lui KS, 2006 "DELPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks",In Proceeding of International Symposium on Wireless Pervasive Computing, pp. 6-11.

[5] 5. Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, Nov. 2008 "Analysis of wormhole Intrusion Attacks In MANETS",IEEE Military Communications Conference,MILCOM 2008.

[6] 6. Y.-C. Hu, A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, Security and Privecy Magazine, IEEE, vol. 2, issue 3,pp. 28-39, May 2004.

[7] 7. R. S. Khainwar, A. Jain , J. P. Tyagi , Dec 2011 ,"Elimination of Wormhole Attacker Node in MANET Using Performance Evaluation Multipath Algorithm " International Journal of Egineering Technology and Advanced Engineering, Volume 1, Issue 2, pp. 40-47.

[8] 8. F. Natt-Abdesselam, B. Bensaou, T. Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Network", IEEE Communications Magazine, 46(4), pp. 127-133, 2008.

[9] 9. M.A. Gorlatva, P. C. Mason, M. Wang, L. Lamont, R. Liscano, "Detecting Wormhole attacks in Mobile A d Hoc Networks through Protocol Breaking and Packet Timing Analysis", In IEEE Military Communications Conference, pp. 1-7 ,2000

[10] 10. Shalini Jain, Dr.Satbir Jain, " Detection and prevention of wormhole attack in mobile adhoc networks" , In Proceedings of the International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010, pp.78-86.

[11] 11. Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. pp. 2-17.

