ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

A CROSS LAYER MAC PROTOCAL FOR WORM HOLEDETECTION ANDOPTIMIZED PIPLINED DATA FLOW IN NETWORK

P.PADMA PRIYA, M.E,Final year
Dept. of Computer Science and Engineering
Mahendra Engineering College (Autonomous)
Namakkal Dt., India.

R.SATHISH KUMAR,M.E.,,,Asst.professor
Dept. of Computer Science and Engineering
Mahendra Engineering College (Autonomous)
Namakkal Dt.

***Abstract*—A MANET (Mobile Ad Hoc Network) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. This cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to attack node behavior. Thus, the overall network performance could be seriously affected. The use of worm hole is a well-known mechanism to detect attack nodes. However,the detection process performed by worm hole can fail, generating false positives and false negatives that can induce to wrongoperations.**

Moreover, relying on local worm hole alone can lead to poor performance when detecting attack nodes, in terms of precision and speed. This is especially important on networks with sporadic contacts, such as Delay Tolerant Networks (DTNs), where sometimes worm hole lack of enough time or information to detect the attack nodes. Thus, propose a cross layer mac protocol as a collaborative approach based on the diffusion of local attack nodes awareness when a contact occurs, so that information about attack nodes is quickly propagated. This collaborative approach reduces the time and increases the precision when detecting attack nodes.

***Keywords— Cross mac layer, MANET, 4D continuous time Markov chain*, false positive, false negative.**

I. INTRODUCTION

MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form a random topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human induced disasters, military conflicts, emergency medical situations etc.

MANETs are autonomous and decentralized networks. So, they can operate no matter which nodes are connected or not connected to the network. Connectivity of nodes only affects the topology and routing of the network, not the general operations. Since, MANETs don't have any centralization, operations are done distributed, so

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

each node has to have sufficient information about the network and have to operate independently.

Two nodes that want to communicate with each other can send and receive messages directly, if they are both in their transmission range. Otherwise, every node is also capable to be a router, and the messages between nodes are relayed by the intermediate nodes, from the originator of the message to the destination. Since the nodes are mobile and the members of the network changes without any notice, the network structure is very dynamic. So, the route the messages are sent by, are dynamic also.Routing is a very vital and performance critic issue for ad hoc networks.

II. LITERATURE SURVEY

A. *Enforcing Service Availability in Mobile Ad-Hoc WANs:*

Enforcing Service Availabilityaddress the problem of service availability in mobile ad-hoc WANs. A secure mechanism to stimulate end users to keep their devices turned on, to refrain from overloading the network, and to thwart tampering aimed at converting the device into a "attack" one is implemented. The solution is based on the application of a tamper resistant security module in each device and cryptographic protection of messages.Communication among users is based on packet switched1, multi-hop, wireless communication of voice and data. An important characteristic of terminode networks is that there are no routing tables stored in the devices. Instead, a simple packet forwardingmechanism lets each of the terminodes located on the route of a given packet compute the "best" next hop toward the final destination.

All networking services (e.g., packet forwarding, mobility management) should be provided by the terminodes themselves, these services are available only if the terminodes (or, more precisely, their users) are willing to provide them. On the other hand, service provision is not in the direct interest of users, because it consumes energy and thus, reduces battery lifetime. Therefore, a stimulation mechanism that encourages users to leave their terminodes switched on and let them provide services to other terminodes is required. One can say that being able to receive messages is enough motivation for the user to leave her terminode switched on. While this may indeed be true, it is certainly not enough to encourage users to provide services to other terminodes. The hardware and the software of the terminode can be tampered with and their behavior can be modified by the user in a way that the device can receive messages but it does not provide any services to the community. Furthermore, criminal organizations can tamper with terminodes and sell corrupted devices, which do not co-operate in order to save energy, on a large scale.

B. *Self-Policing Mobile As-Hoc Networks by Reputation Systems:*

Node misbehavior due to attack or malicious reasons or faulty nodes can significantly degrade the performance of mobile ad-hoc networks. Christo Ananth et al. [10] discussed about a system,the effective incentive scheme is proposed to stimulate the forwarding cooperation of nodes in VANETs. In a coalitional game model, every relevant node cooperates in forwarding messages as required by the routing protocol. This scheme is extended with constrained storage space. A lightweight approach is also proposed to stimulate the cooperation. Here explain in particular how it is possible to use second-hand information while mitigating contamination by spurious ratings.

C. *Observation-based Cooperation Enforcement in Ad-Hoc Networks:*

Ad hoc networks rely on the cooperation of the nodes participating inthe network to forward packets for each other. A node may decide not to cooperate to save its resources while still using the network to relay its traffic. If too many nodes exhibit this behavior, network performance degrades and cooperating nodes may find themselves unfairly loaded. If a node observes another node not participating correctly, it reports this observation to other nodes who then take action to avoid being affected and potentially punish the

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

bad node by refusing to forward its traffic. Unfortunately, such second-hand reputation information is subject to false accusations and requires maintaining trust relationships with other nodes.The objective of OCEAN is to avoid this trust-management machinery and see how far can get simply by using direct first-hand observations of other nodes' behavior. We find that, in many scenarios, OCEAN can do as well as, or even better than, schemes requiring second-hand reputation exchanges. This encouraging result could possibly help obviate solutions requiring trust-management for some contexts.

OCEAN considers two types of routing misbehavior. The first, which we call misleading, is that a node may respond positively to route requests but then fail to forward the actual packets, misleading other nodes into unsuccessfully sending their traffic through it. Previous approaches at mitigating misleading routing misbehavior require nodes in the network to exchange reputation information about other nodes. If a node observes another node participating incorrectly, it reports this observation to other nodes who then take action to avoid being affected by the misbehavior and perhaps even punish the node by refusing to forward its traffic.

III. Existing System

Worm hole are appropriate mechanisms to detect misbehaving and attack nodes. Essentially, cross mac systems overhear wireless traffic and analyze it to decide whether neighbor nodes are behaving in aattack manner (i.e. a) motivation or incentive based approaches, and b) detection and exclusion). When the cross mac detects aattack node it is marked as a positive detection (or a negative detection, if it is detected as a non attack node). Nevertheless, worm hole can fail on this detection, generating false positives and false negatives that seriously degrade the behavior of the system.

Another source of problems for cooperative approaches is the presence of colluding or malicious nodes. In this case, the effect can even be more harmful, since these nodes try to intentionally disturb the correct behavior of the network. Malicious nodes are hard to detect using worm hole, as they can intentionally participate in network communication with the only goal to hide their behavior from the network.

IV. Proposed System

Piplined Data Flow In Network Cross Mac as a new scheme for detecting attack nodes that combines local cross mac detections and the dissemination of this information on the network. If one node has previously detected aattack node it can transmit this information to other nodes when a contact occurs. This way, nodes have second hand information about the attack nodes in the network. The goal of our approach is to reduce the detection time and to improve the precision by reducing the effect of both false negatives and false positives.

To evaluate the efficiency of Piplined Data Flow In Network, first introduce an analytical performance model. The network as a Continuous Time Markov Chain (CTMC) and derive expressions for obtaining the time and overhead (cost) of detection of attack nodes under the influence of false positives, false negatives and malicious nodes. In general, the analytical evaluation shows a significant reduction of the detection time of attack nodes with a reduced overhead when comparing piplined data flow in network against a traditional cross mac. The impact of false negatives and false positives is also greatly reduced. Finally, the pernicious effect of malicious nodes can be reduced using the reputation detection scheme. Also evaluate PIPLINED DATA FLOW IN NETWORK with real mobility scenarios using well known human and vehicular mobility traces. These experimental results confirm that the approach is very efficient. Thus, we propose the system to be in a globalization method.

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

V. SYSTEM DESIGN

A. Model for PIPLINED DATA FLOW IN NETWORK Architecture:

Aattack node usually denies packet forwarding in order to save its own resources. This behaviour implies that aattack node neither participates in routing nor relays data packets. A common technique to detect this attackbehaviour is network monitoring using local worm hole. A node's cross mac consists on overhearing the packets transmitted and received by its neighbours in order to detect anomalies, such as the ratio between packets received to packets being re-transmitted. By using this technique, the local cross mac can generate a positive (or negative) detection in case the node is acting attackly (or not).

It is based on the combination of a local cross mac and the diffusion of information when contact between pairs of nodes occurs. A contact is defined as an opportunity of transmission between a pair of nodes (that is, two nodes have enough time to communicate between them). Assuming that there is only one attack node, the figure shows how initially no node has information about the attack node. When a node detects aattack node using its cross mac, it is marked as a positive, and if it is detected as a non attack node, it is marked as a negative. Later on, when this node contacts another node, it can transmit this information to it; so, from that moment on, both nodes store information about these positive (or negative) detections.Therefore, a node can become aware about attack nodes directly (using its cross mac) or indirectly, through the collaborative transmission of information that is provided by other nodes.

Thediffusionmodulecangenerateindirectev entswhenacontactwith neighbournodesoccurs. Nevertheless,acontactdoes notalwaysimply collaboration,sowemodel this probabilityofcollaboration.Thedegreeofcollabor ationisaglobalparameter,anditisused toreflectthateither amessagewith theinformationabouttheattack node is lost, or that a node temporallydoes not collaborate (for example,due toafailure orsimply because itisswitched off).In real networks,full collaborationisalmost impossible.

B. Malicious Nodes and attacker model

Malicious nodes attempt to attack the PIPLINED DATA FLOW IN NETWORK system by generating wrong information about the nodes. Thus, the attacker model addresses the behavior or capabilities of these malicious nodes. A malicious node attack consists of trying to send a positive about a node that is not aattack node, or a negative about aattack node, with the goal of producing false positives and false negatives on the rest of nodes. In order to do this, it must have some knowledge about the way PIPLINED DATA FLOW IN NETWORK works. The effectiveness of this behavior clearly depends on the rate and precision that malicious nodes can generate wrong information. Malicious nodes are assumed to have a communications hardware similar to the rest of nodes, so they can hear all neighbour messages in a similar range than the rest of nodes. Nevertheless, the attacker could use high-gain antennas to increase its communications range and thus disseminate false information in a more effective manner.

Regarding the diffusion of information on the network, our approach does not assume any security measures, such as message ciphering or node authentication. Nevertheless, if these measures exist, the effect of malicious nodes in PIPLINED DATA FLOW IN NETWORK will be greatly reduced or even non-existent.Thus, we assume that malicious nodes can be active, and use this information in order to generate false positives/negatives about other nodes.

C. Detection of Attack Nodes:

Mobile wireless network, capable of autonomous operation operates without base station or infrastructure. In this network nodes cooperate with each other to provide connectivity and operate without centralized administration. A node is called attack if it drops packets of others due to either

All Rights Reserved © 2016 IJARTET

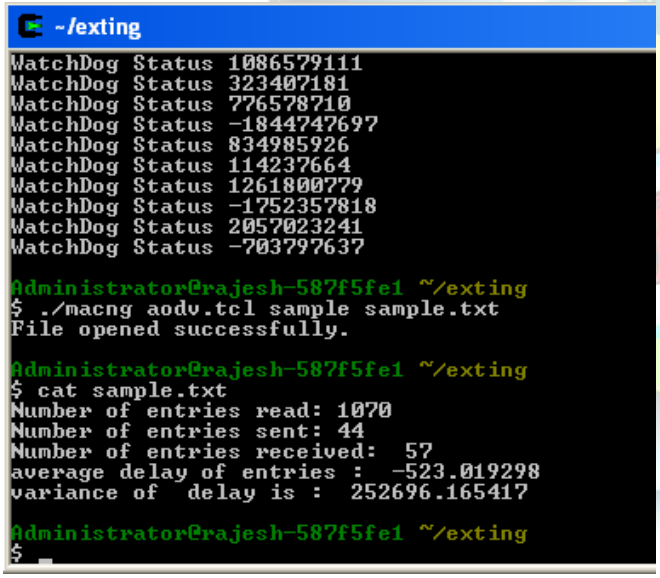
ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

honest causes such as collisions, channel errors, or buffer overflows or maliciously such as to save its energy or bandwidth, black hole or wormhole attack, network congestion. Aattacknode degrades efficiency of packet transfer and accelerates the packet delivery time and packet loss rate and finally creates Network Partitioning**.**

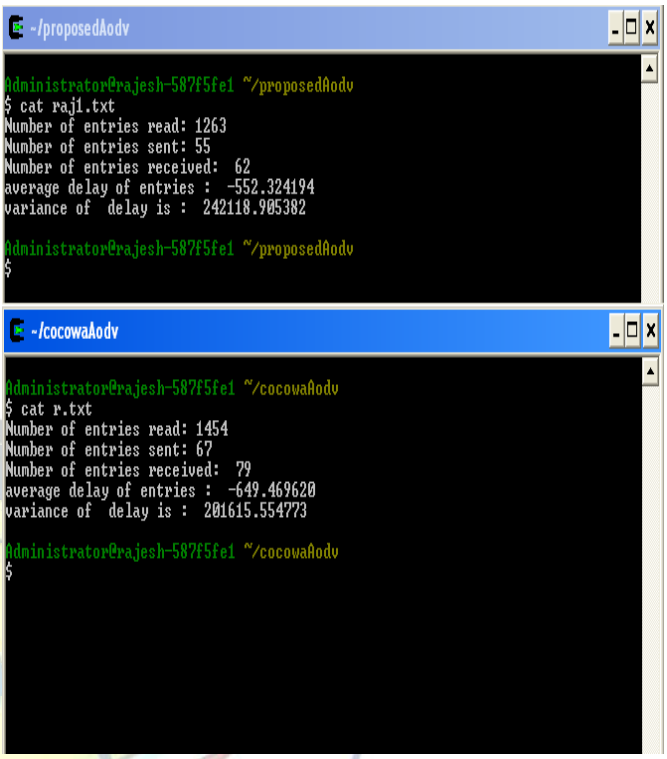
D. Detection of False Positive:

This model evaluates how fast a false positive spreads in the network (the diffusion time). Thus, in this case, a greater diffusion time stands for a lower impact of false positives. The diffusion time is similar to the detection time of true positivesdescribed in the previous subsection, and it can be obtained in a similar way.

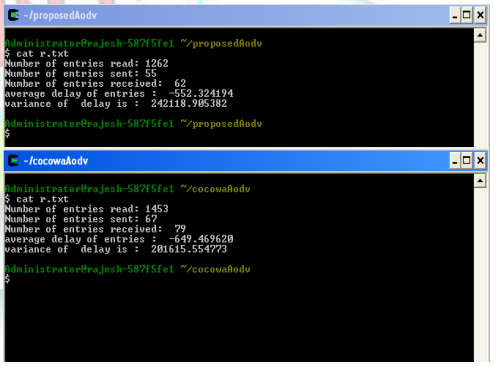
VI. EXPERIMENTAL EVALUATION



A Sample data traffic in the MANET for 40 nodes



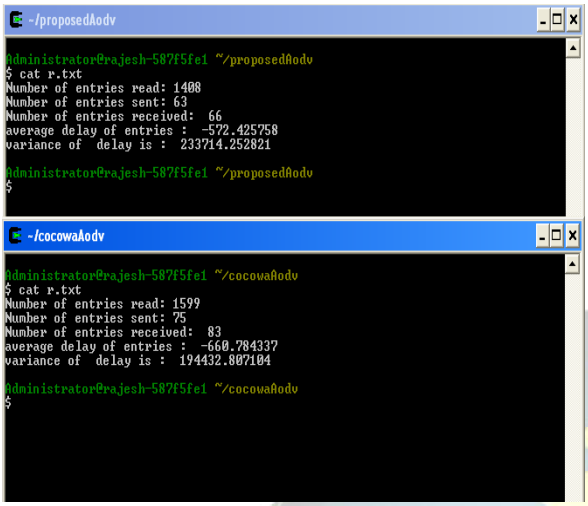
Comparison of 1 blackhole attack in region of 40 nodes



Comparison of 2 balckhole attacks in the region of 40 nodes

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016



Comparison of 8 balckhole attacks in the traffic

VII. CONCLUSION

PIPLINED DATA FLOW IN NETWORK as a collaborative contact-based cross mac is used to reduce the time and improve the effectiveness of detecting attack nodes, reducing the harmful effect of false positives, false negatives and malicious nodes. PIPLINED DATA FLOW IN NETWORK is based on the diffusion of the known positive and negative detections.This reduction is very significant, ranging from 20 percent for very low degree of collaboration to 99 percent for higher degrees of collaboration. Finally, using PIPLINED DATA FLOW IN NETWORK the effect of malicious or collusive nodes can reduce. In short, the combined effect of collaboration and reputation of the approach can reduce the detection time while increasing the global accuracy using a moderate local precision cross mac.

ACKNOWLEDGEMENT

We would like to extend our esteemed thanks to our Project Co-ordinatorDr.B.GOMATHY, Assistant Professor (Senior Grade), Department of Computer Science and Engineering and to our guide Ms.S.VARUNA, Assistant Professor, Department of Computer Science and Engineering for their valuable initiation, motivation, continuous guidance and much needed technical support extended for us to complete the project.

REFERENCES

[1] L. Buttyan and J.-P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in Proc. 1st Annu. Workshop Mobile Ad Hoc Network Computing., pp. 87–96, 2000

[2] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on opportunistic forwarding algorithms," IEEE Transaction of Mobile Computing., vol. 6, no. 6, pp. 606–620, 2007.

[3] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks", 2003.

[4] J. R. Douceur, "The sybil attack," in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., pp. 251–260, 2002.

[5] S. Abbas, M.Merabti,D.Llewellyn-Jones, and K.Kifayat, "Lightweight sybilattack detectionin manets," IEEE Syst. J., vol.7,no.2,pp.236–248,2013.

[6] S.Bucheggerand J.-Y. LeBoudee, "Self-policing mobile ad-hoc networks by reputation systems," IEEECommunications.Mag., vol. 43, no.7,pp.101–107, 2005.

[7] W.Gao, Q.Li,B.Zhao, and G.Cao, "Multicasting in delay tolerant networks: A social network perspective, "in Proc.10th ACMInstitute Symposium. Mobile Ad Hoc Network Computing.,pp.299–308, 2009.

[8] R.Groenevelt, P. Nain, and G. Koole, "The message delay in mobile ad hoc networks," Perform. Evaluation, vol. 62,pp. 210–228, 2005.

[9] E.Hernandez-Orallo, M.D.Serrat, J.-

All Rights Reserved © 2016 IJARTET

C.Cano, C.M.T.Calafate, and P.Manzoni, "Improving attack node detection in MANETsusing a collaborative cross mac," IEEE Communications Letter.,vol.16,no.5, pp.642–645, 2012.

[10] Christo Ananth, M.Muthamil Jothi, A.Nancy, V.Manjula, R.Muthu Veni, S.Kavya, "Efficient message forwarding in MANETs", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1,Issue 1, August 2015,pp:6-9

[11] M.Hollick, J.Schmitt, C.Seipl and R. Steinmetz, "On the effect of node misbehaviourin ad hoc networks,"in ProceedingsIEEEInstitute of Conference Communications.,pp.3759–3763, 2004.

[12] Y.Zhang,W.Lee,andY.A.Huang,"Intrusio ndetectiontechniquesformobile wirelessnetworks,"WirelessNetwork.,vol. 9,no.5, pp.545–556, 2005.

[13] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modelling of epidemic routing," Computer Network., vol. 51, no. 10, pp. 2867–2891, 2007.

All Rights Reserved © 2016 IJARTET