International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
(Volume 28, Issue 03) Publishing Month: August 2017
An Indexed and Referred Journal with Impact Factor: 2.75
ISSN: 2347-601X
www.ijemhs.com

Fellowship Model against Black Hole Attacks in MANET: New Node Monitoring

[1]Arpita Priyadarsinee
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India
[2]Swetapadma Sahu
Maharaja Institute of Technology, Bhubaneswar, Odisha, India

Abstract

In mobile ad-hoc network one of the vulnerable threat is the security issues ad in the absence of any centralized controller, now a day's these issues are increasing at a high speed. The packet drop attacks are one of those attacks which degrade the network performance. This paper describes a novel node monitoring mechanism with a fellowship model against packet drop attacks by setting up an observance zone where suspected nodes are observed for their performance and behavior. Threshold limits are set to monitor the equivalence ratio of number of packets received at the node and transmitted by node inside mobile ad hoc networks. The proposed fellowship model enforces a binding on the nodes to deliver essential services in order to receive services from neighboring nodes thus improving the overall network performance.

Keywords: Black-hole attack, equivalence ratio, fair-chance scheme, observance zone, fellowship model.

1. INTRODUCTION

Mobile ad-hoc networks are infrastructure less and self organized or configured network of mobile devices connected with radio signals. There is no centralized controller for the networking activities like monitoring, modifications and updating of the nodes inside the network as shown in figure 1. Each node is independent to move in any direction and hence have the freedom to change the links to other nodes frequently. There have been serious security threats in MANET in recent years. These usually lead to performance degradation, less throughput, congestion, delayed response time, buffer overflow etc. Among them is a famous attack on packets known as black-hole attack which is also a part of DoS(Denial of service) attacks. In this, a router relays packets to different nodes but due to presence of malicious nodes these packets are susceptible to packet drop attacks. Due to this, there is hindrance is secure and reliable communication inside network.

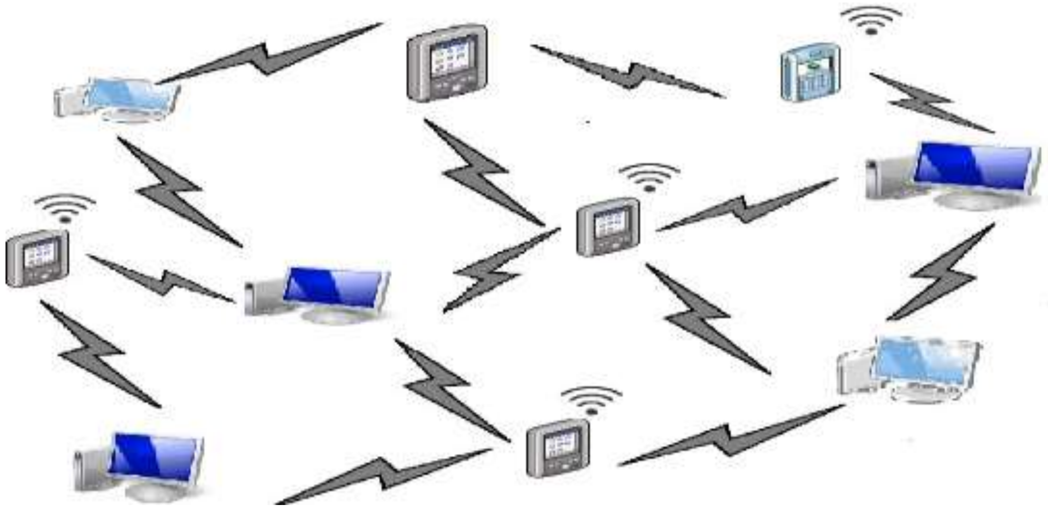

Figure 1. MANET Scenario

Section 2 addresses the seriousness of packet drop attacks and related work done so far in this area. Section 3 elaborates our proposal and defending scheme for packet drop attacks. Section 4 provides concluding remarks.

2. LITERATURE SURVEY

The packet drop loss in ad-hoc network gained importance because of self-serving nodes which fail to provide the basic facility of forwarding the packets to neighboring nodes. This causes an occupational hazard in the functionality of network. Generally there are two types of nodes- selfish and malicious nodes. Selfish nodes are those nodes which act in the context of enhancing its performance while malicious nodes are those which mortifies the functions of network through its continual activity. The WATCHERS [1] from UC Davis was presented to detect and remove routers that maliciously drop or misroute packets. A WATCHER was based on the “principle of packet flow conservation”. But it could not differentiate much between malicious and genuine nodes. Although it was robust against byzantine faults, it could not be much effective in today’s internet world to reduce packet loss. The basic mechanism of packet drop loss is that the nodes do not progress the packets to other nodes selfishly or maliciously. Packet Drop loss could occur due to Black hole attack. Sometimes the routers behave maliciously i.e. the routers do not forwards packets, such kinds of attacks are known as “Grey Hole Attack”. In case of routers, the attacks can be traced quickly while in the case of nodes it’s a cumbersome task. Many researchers have worked in this field and have tried to find solutions to this attack [2-6]. Energy level was one of the parameter on which the researchers have shown their results. This idea works on the basis of the ratio of fraction of energy committed for a node, to overall energy contributed towards the network. The node is retained inside the network on the basis of energy level and the energy level is decided by the activeness of node in a network through mathematical computations. Mathematical computations are [7] too complicated to clench and sometimes the results are catastrophic. It can be said that the computations are accurate but they are very much prone to ambiguity in the case of ad-hoc networks. Few techniques involve usage of routing table information which is modified after detecting the MAC address of malicious node which uses jamming style DoS attack to cease their activities [8]. Another approach to reduce attacks was using historical evidence trust management based strategy. [9] Direct trust value (DTV) was used amongst neighboring nodes to monitor the behavior of nodes depending on their past against black hole attacks. However, there is high possibility that trust values may get compromised by the malicious nodes. Also the third party used for setting the trust values is also vulnerable to attacks. Recent methods included an [10] introduction to a new protocol called RAEED (Robust formally Analyzed protocol for wireless sensor networks Deployment) which reduces this attack but not by a considerable percentage. To overcome the issues faced in order to implement these strategies there is a need of an effective mechanism to curb these attacks and make network more secure.

3. PROPOSED APPROACH

In this paper, we put forth a mechanism to reduce these packet-drop attacks by implementing "*node monitoring with fellowship*" technique. We introduce an obligation on the nodes inside a particular network to render services to network. If services are not rendered, the node will be expelled outside the performance. However, we have kept a "*fair-chance*" scheme for all nodes which help to make out whether it is genuine node or malicious node.

Fellowship of Network

The prime parameter we used in this to address packet drop attacks issue is by maintaining the count of incoming packets, except the destined one on that node and the count of outgoing nodes except the ones which are originated at that node, should be same, referred to as "*equivalence ratio*". If that count is same, there is uniform distribution and forwarding of packets among the nodes inside network. However, if the count is not same, then that particular node is kept under "*observance zone*" in order to monitor its suspicious behavior. We suggest a periodical reporting of all nodes about their *equivalence ratio* to neighboring nodes inside the network.

This will help to decide whether to keep a particular node in "*observance zone*" which could be done with polling techniques amongst each other. Inside, *observance zone*, the suspected node is given "*fair-chance*" treatment. That is, during *observance zone* period, the suspected node is required to submit its "*status- message*" to neighboring nodes to prove its genuineness of performance inside network. The genuine nodes will promptly provide their status-message to neighboring nodes because they will be willing to stay inside the network to render services under obligation for the network. However, the malicious nodes may or may not reply their status-messages to neighboring nodes since they have to degrade performance of network. But, for such *status-messages* only *fair-chance* is given. That is, a standard threshold level is been set up unanimously amongst neighboring nodes inside network. *Status-messages* will be entertained only up to threshold level. So, even if malicious nodes produce and fake their own status-messages to neighboring nodes in order to sustain inside network due to threshold limits it will not degrade network performance much. When threshold is crossed, the neighboring nodes will be intimated about the node which is under *observance zone* and a unanimous decision will be taken to expel that suspected node out of the network. Because of this scheme, there is possibility that the suspected node is expelled outside the network under 2 circumstances: either its genuine node (which are underperforming) or malicious nodes. In both cases, the suspected node needs to be expelled out of network because it is leading to performance degradation of the network. The "*fair-chance*" scheme ensures that genuine nodes are given fair chance to justify themselves and repair itself soon to prove their genuineness to render services to network under obligation.

Scenario Assumptions

Let the nodes inside MANET be connected through wireless links with each other. Let number of packets be transmitted and received with each other by the nodes. Let nodes be named alphabetically from A,B,C…and so on till Z. Let node X be malicious node which drops packets and undergoes black hole attack and hence has poor *equivalence ratio* while node Y be the genuine node but has poor *equivalence ratio* due to network congestion or may be due to some other network issues. All nodes inside the network follow the principle of "*node monitoring with fellowship".* Data structures used are the networking parameters which are as follows:

1)*equi_ratio* = denoting the *equivalence_ratio* of nodes

2)*observance_zone*= denoting list of suspected nodes inside *observance zone*. 3)*threshold_value*= denoting *threshold value* decided by the nodes inside MANET.

4)*status_message*= denoting the status messages exchanged amongst neighboring nodes.

Steps involved:

Step 1: All nodes calculate their own *equivalence ratio(equi_ratio)* and share it with their neighboring nodes(let them be at one hop distance) periodically.

Step 2: All nodes unanimously agree upon a standard threshold level (in this case, *threshold_value*=3) through exchange of messages using agreement protocols.

Step 3: All nodes will monitor their neighbor's *equi_ratio* and if any node has *equi_ratio* which is quite poor then that particular node will be kept under "*observance zone*" list through mutual exchange of messages of nodes inside network. These nodes may be suspected as malicious nodes or genuine nodes but with poor performance.

Step 4: Once the suspected node is kept in "*observance zone*" list, it is made mandatory for that node to report the "*status_message*" to the neighboring nodes to justify their performance and behavior.

Step 5: If it's a malicious node (node X) it may either fake its *status_message* to show its genuineness and stay inside network or it may just avoid sending its *status_message* since it wishes to continue its malicious activities in future too. If it is genuine node (node Y) it will send *status_message* in order to prove its genuineness and try to improve its performance by repairing itself with the network issues it is facing while sending the packets.

Step 6: Thus, the nodes which cross the limits *of threshold_value*, will be immediately expelled outside the network through exchange of protocols and messages between the neighboring nodes. In this way, packet-drop attacks can be considerably reduced. Figure 2 explains the workflow mechanism.

Advantages:

1. Fair chance scheme ensures genuineness of innocent nodes.
2. No complex mathematical computations of energy levels at each node.
3. Periodical reporting ensures removal of both underperforming and malicious nodes from the network.
4. Up gradation of network performance in MANET.

Disadvantages

However, there is an overhead of exchanging more number of messages among the neighboring nodes. Optimization on number of messages exchanged during communication can be addressed and worked upon in future research.

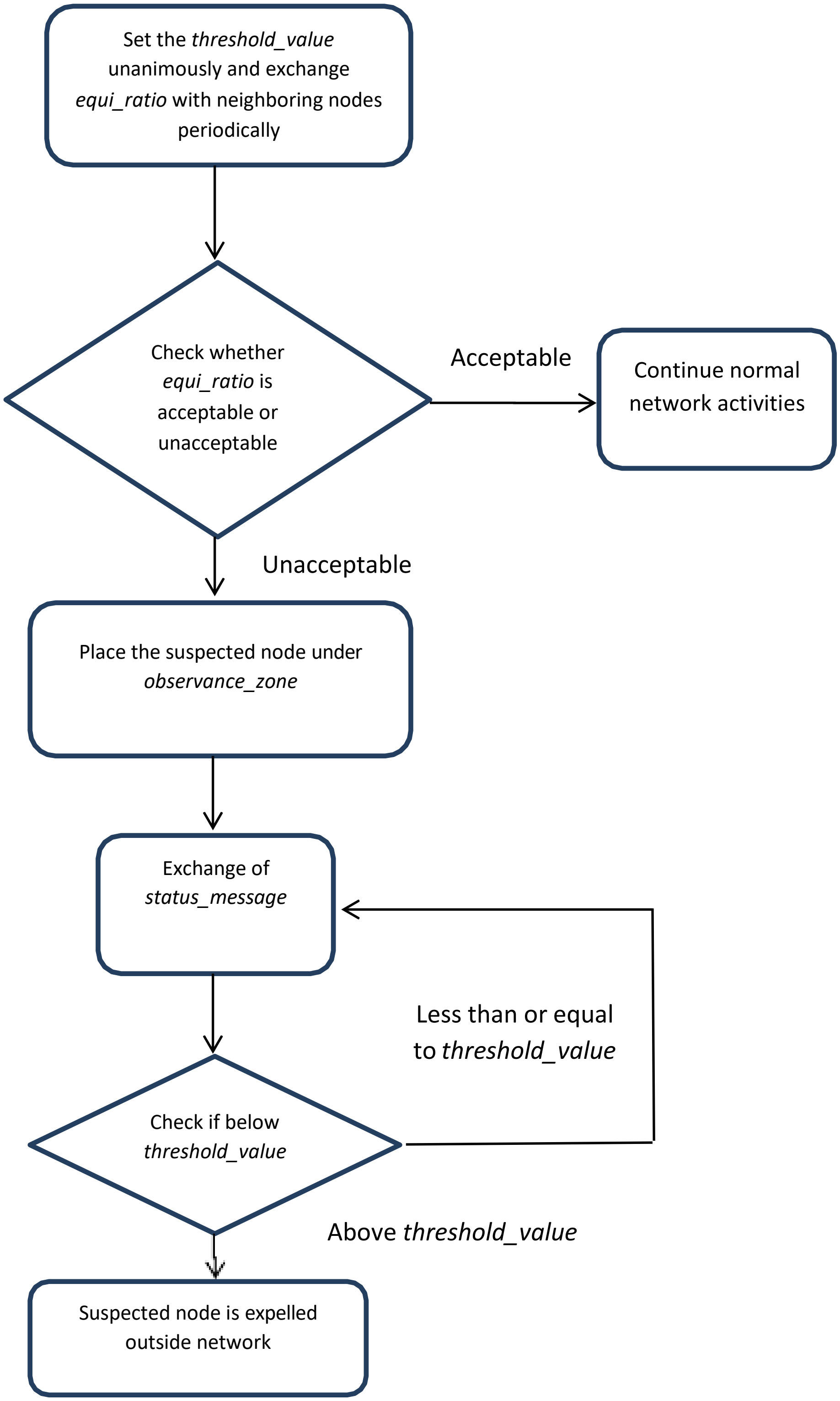
Set the *threshold_value* unanimously and exchange *equi_ratio* with neighboring nodes periodically
Check whether *equi_ratio* is acceptable or unacceptable
Acceptable
Continue normal network activities
Unacceptable
Place the suspected node under *observance_zone*
Exchange of *status_message*
Less than or equal to *threshold_value*
Check if below *threshold_value*
Above *threshold_value*
Suspected node is expelled outside network

Figure 2. Flowchart of proposed mechanism

4. CONCLUSION

In this paper, we have proposed a novel scheme to reduce packet drop attacks and enhance the network performance. However, we anticipate our "node-monitoring with fellowship" model may lead to increase in number of exchanged messages amongst neighboring nodes during the agreement protocols inside network but at the same time it will be robust against attacks and thus increase the availability of nodes in mobile ad-hoc networks. The outcomes of minimizing packet drop loss have better utility of channel, resources and QoS guaranteed which results in productive priority management and a considerable controlled traffic by periodic surveillance over nodes. The future research on this would be to reduce the exchange of messages amongst the nodes, minimize the overhead and achieve optimization inside mobile ad-hoc networks.

REFERENCES

[1] K. A. Bradley, S. Cheung, N. Puketza, B. Mukherjee and R. A. Olsson, *Detecting Disruptive Routers: A Distributed Network Monitoring Approach*, in the 1998 IEEE Symposium on Security and Privacy, May 1998.

[2] Y.C. Hu, A. Perrig and D. B. Johnson, *Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks*, presented at International Conference on Mobile Computing and Networking, Atlanta, Georgia, USA, pp. 12 - 23, 2002.

[3] P. Papadimitratos and Z. J. Haas, *Secure Routing for Mobile Ad hoc Network*s, presented at SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX, January2002.

[4] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields and E. M. Belding-Royer, *A Secure Routing Protocol for Ad Hoc Networks*, presented at 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, pp. 78 - 89, 2002.

[5] V. Balakrishnan and V. Varadharajan, *Designing Secure Wireless Mobile Ad hoc Networks*, presented at Proceedings of the 19th IEEE International Conference on advanced information Networking and Applications (AINA 2005). Taiwan, pp. 5-8, March 2005.

[6] V. Balakrishnan and V. Varadharajan, *Packet Drop Attack: A Serious Threat to Operational Mobile Ad hoc Networks*, presented at Proceedings of the International Conference on Networks and Communication Systems (NCS 2005), Krabi, pp. 89-95, April 2005.

[7] Venkatesan Balakrishnan and Vijay Varadharajan *Short Paper: Fellowship in Mobile Ad hoc Networks* presented at Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05) IEEE.

[8] Raza, M., and Hyder, S.I. *A forced routing information modification model for preventing black hole attacks in wireless Ad Hoc network* presented at Applied Sciences and Technology (IBCAST), 2012, 9th International Bhurban Conference, Islamabad, pp. 418-422, January 2012.

[9] Bo Yang , Yamamoto, R., Tanaka, Y. *Historical evidence based trust management strategy against black hole attacks in MANET* published in 14th International Advanced Communication Technology(ICACT), 2012 on pp. 394 – 399.

[10] Saghar, K., Kendall, D.and Bouridane, A. *Application of formal modeling to detect black hole attacks in wireless sensor network routing protocols* .Applied Sciences and Technology (IBCAST), 2014, 11th International Bhurban Conference, Islamabad, pp. 191-194, January 2014.