A Comparitive Study of Malicious Node Detection Scheme in MANET

Ms. N.U. Tharini[1], **Ms. K. Devipriya**[2]

Dept of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India[1,2]

Abstract: A mobile ad hoc network (MANET) is the continuously self-configuring, infrastructure less network of mobile devices connected without the wires and sometimes untrustworthy. Mobile ad-hoc networks (MANETs) assumes that mobile nodes voluntary cooperate in order to work properly. This type of cooperation is a cost-intensive activity and some of the nodes can refuses to cooperate leading to selfish node behavior. Thus an overall network performance could be seriously affected. The use of Watchdog is a well-known mechanism to detect the threats and attacks from misbehaved and selfish nodes in computer networks. In infrastructure less network attack detection and reaction is a key issue to the whole network. Watchdog system overhear traffic and perform analysis using data collected to decide the grade of misbehavior of neighbor nodes present and therefore an accuracy and detection speed plays a key role in achieving the right level of network security and performance. The problem behind the use of watchdog is that they can cause a relatively high level of false positives, false negatives and causes black hole attack. This paper proposes a collaborative approach for detecting black holes and selfish nodes in manet using a set of watchdog which collaborate to enhance their individual and collective performance and shows that using this approach the detection time of misbehaved nodes is reduced and an overall accuracy is increased.

Keywords: Mobile Ad hoc Networks (MANET), selfish, node, misbehavior, detection.

I. INTRODUCTION

Mobile Ad Hoc Network (MANETs) has become one of the most prevalent areas of research in the recent years and because of the challenges it pose to the related protocols. MANET is a new emerging technology which enables the users to communicate without any physical infrastructure regard less of their geographical location. Mobile Ad Hoc Network, usually known as MANET, consists of a set of wireless mobile nodes that functions as a network in an absence of any kind of centralized administration and networking infrastructure. These types of networks rely on cooperation of their nodes to correctly work that is every network node generate and send its own packets and forward packets in behalf of the other nodes.

When MANET is deployed we have to assume that there could be a percentage of misbehaved nodes. The type of misbehaved nodes, their number, and their

Positions and the movement patterns are the key issues which deeply impact the mobile ad hoc network performance [8]. Additionally network performance will be drastically reduced if nothing is done to cope with these threats. To the end an effective protection against misbehaved nodes will be mandatory to preserve the correct functions of the MANET [6].

In MANET there are basically two kinds of packet flows: data packet flow and route maintenance packet flow. However not all misbehaved nodes have the same impact on the network performance due to the type of packet flows they affect. Really malicious node will damage the network, spoofing routes, flooding the wireless channel and carrying out a man-in-the-middle attack. These are classical attacks that every network could suffer and a solution has been devised for them. All types of misbehaved nodes, selfish and malicious have a common behavior: they do not participate in forwarding activities thus being characterized as black holes. A black hole attack is a type of attack in which node intends to disrupt the communication with its neighborhood by attracting all traffic flows in the network and then dropping all packets received without forwarding them to their final destination [5]. To avoid or significantly reduce this type of attack in MANETs, several proposed approaches are based on monitoring the traffic heard by every node to detect the misbehaved nodes and then taking the appropriate actions to avoid a negative effect of that misbehavior [10].

The main problem that arises at this point is to detect the black holes avoiding as much as possible wrong diagnostics like false positives or false negatives. A false positive appears when selected technique identifies the well-behaved node as a misbehaved node. False negative appears when the technique cannot detect a misbehaved node so the network believes that it is normal node when it's potentially disruptive effect. So the accuracy and detection speed are critical issues when design an approach for black holes detection in MANET. Several solutions have been proposed for detecting and isolating misbehaved nodes in MANETs. Marti et al. [7] proposed watchdog and DSR protocol to detect non-forwarding nodes, maintaining the rating for every node and selecting routes with a highest average node rating. The response modules of this technique only relieve misbehaved nodes from forwarding the packets but they continue in getting their traffic forwarded across the network. Buchegger and

Le Boudec [1] proposed CONFIDANT protocol over DSR which combines a watchdog, reputation system, Bayesian filters and information obtained from a node and its neighbors to accurately detect the misbehaved nodes. The system is response to isolate those nodes from the network, punishing them indefinitely. Every node has a credit counter which will be increased when a node forwards packets and decreased when a node send his own packets. When a node has no nuglets, it cannot send its packets so it is the motivation for nodes to forward packets for the network benefit. Zhong et al. [11] proposed SPRITE a credit-based system to incentivize the participation of selfish nodes in MANET communication. It is based on Central Clearance System which charges or gives credit to nodes when they sends or forwards a message. So if a node wants to send a message it must have sufficient credit to do it and that credit is earned by forwarding message to other nodes. The response module of this method is integrated to the incentivation method so that if a node does not forward other nodes message it will not have a credit to send its own messages.

In this work a collaborative contact based watchdog has been proposed which integrates techniques from reputation systems and Bayesian filtering, and makes extensive use of the collaborative nature of MANET. This watchdog will be considered as an Intrusion Detection Systems (IDS) which is a software piece that collects and analyze the network traffic to detect a set of attacks. In this context an intrusion detection systems aim at monitoring the activity of the node in the network in order to detect the misbehavior [5]. Usually, these kinds of software products are built using two building blocks: a Detection or sensor modules, watchdogs, and Response module.

This paper is structured as follows. The summary of the related work of malicious node detection is elaborated in section II. This is followed by a detailed description of detection of malicious node in section III. Then the comparative analysis of malicious node detection methods is provided in section IV. Section V concludes with suggesting the extension of proposed work.

II. RELATED WORK

To the best of our knowledge there are three papers addressing the problem of noncooperation nodes in mobile ad hoc network. The authors of [13] consider the case in which some of the malicious nodes agree to forward packets but it fails to do so. In order to cope with this problem they proposed a mechanism: a watchdog in charge of identifying the misbehaving node. This paper shows that these two mechanisms make it possible to maintain a total throughput of the network at an acceptable level even in the presence of high amount of misbehaving nodes. However the problem is that the selfishness of the node does not seems to be castigated on the contrary by the combination of watchdog and the path rather than misbehaving nodes will not be bothered by the transition of traffic while still enjoying the possibilities to send and to receive packets.

A similar approach to overcome this problem is described in [6]. In that paper the authors propose a protocol called CONFIDANT in which it aims at not only detecting and avoiding but also isolating the misbehaving nodes. The CONFIDANT protocol relies on following components in each Node which identifies deviations from a normal routing behavior a trust manager which send and receive alarm messages to and from other trust manager, a reputation system which rate other nodes according to their observed or reported behavior and the path manager that maintains path ranking and perform specific action when routing messages are processed.

A serious disadvantage of Packet Trade Model is that it allows overloading of the network since the source does not have to pay. At the same time the property of refraining users from overloading the networks is retained. Otherwise the two mechanisms has a very similar flavor just like their protection scheme.

III. MALICIOUS NODE DETECTION SCHEMES

1. Audit Based System

Audit-based system will effectively and efficiently isolates both continuous and selective packet droppers. Yu Zhang and Loukas Lazos [6] proposed a comprehensive system called Audit based Misbehavior Detection (AMD) that will effectively and efficiently isolates both continuous and selective packet droppers. The AMD systems integrate reputation management scheme, trustworthy route discovery and identification of misbehaving node based on the behavioral audits. William Kozma Jr.and Loukas Lazos [7] proposed the novel misbehavior identification scheme called REAct that provides resource efficient account ability for node misbehavior. REAct identifies misbehaving nodes based on their series of random audit triggered upon the performance drop.

2. Reputation Based Systems

Reputation based system use ratings for evaluating the trustworthiness of nodes in the forwarding traffic. These ratings are dynamically adjusted based on the nodes observed behavior. In the context of an ad hoc network Ganeriwal and Srivastava [10] developed a Bayesian model to map binary rating to reputation metric using a beta probability density function. Jøsang and Ismail [11] proposed the similar ranking system that utilized a direct feedback received from one hop neighbors. Michiardi and Molva [12] proposed the CORE mechanism for computing, distributing, and updating reputation value composed of disparate sources of information. Reputation based system use neighboring monitoring technique to evaluate the behavior of nodes. Marti et al. [13] proposed a scheme which relies on two modules the watchdog and path rater. The watchdog module is responsible for overhearing the transmission of successor node thus verifying the successful packet forwarding to the next hop. The path rater module use an accusations generated by the watchdog module to select the path free of misbehaving nodes. Buchegger and Le Boudec [14] proposed a scheme

DOI 10.17148/IJARCCE.2017.6297

called CONFIDANT which extends the watchdog module to all one hop neighbors that can monitor nearby transmissions. When misbehavior is detected, monitoring node broadcast alarm message in order to notify their peers of the detected misbehavior and adjust a corresponding Reputation values. A similar monitoring technique has also been used in. Transmission overhearing becomes highly complex in multi channel network or when nodes are equipped with directional antenna. Neighboring nodes may be engaged in parallel Transmission in orthogonal channel or different sectors thus being unable to monitor their peer. Moreover operating radio in promiscuous mode for the purposes of overhearing requires up to 0.5 times the amount of energy for transmitting the message [12].

3. Acknowledgment Based Systems

Acknowledgment based systems rely on a reception of acknowledgments to verify that the message is Forwarded to a next hop. Balakrishnan et al. [16] proposed a scheme called TWOACK, where nodes explicitly send 2-hop acknowledgment message along the reverse path, verifying that the intermediate node faithfully forwarded packet. A packet that has not yet been acknowledged remains in a cache until they get expire. A value is assigned to the quantity and frequency of unverified packets to determine misbehavior. Liu et al. [13] improved on TWOACK by proposing 2ACK.Similar to 2ACK the node explicitly sends 2-hop Acknowledgment to verify the cooperation. Xue and Nahrstedt [8] proposed the Best effort Fault Tolerant Routing scheme which relies on end to end acknowledgment messages to monitor packet delivery Ratio and select the routing path which avoids the misbehaving node. Awerbuch et al. [11] proposed an on demand secure routing protocol (ODSBR) that identifies misbehaving link. The source probes to intermediate nodes to acknowledge each packet and performs a binary search to identify the links where packets are dropped.

ACK based systems incur a high communication and energy overhead for behavioral monitoring. For each packet transmitted by the source several acknowledgement must be transmitted and received over several hop. Moreover they cannot detect attacks of selective nature over encrypted end to end flow.

4. Distributed Cooperative Mechanism (DCM)

Chang Wu Yu et al. proposes a distributed and cooperative mechanism viz. [10] DCM to solve the collaborative black hole attack. Because the nodes works cooperatively that they can analyze, detect, mitigate multiple black hole attack. The DCM is composed of four sub-modules. In local data collection phase an estimation table is constructed and maintained by each node in the network. Each node evaluates the information of overhearing packet to determine whether there are any malicious nodes. If there is one suspicious node the detected node initiate the local detection phase to recognize whether there is possible black hole node. The initial detection node sends the check packet to ask the cooperative node. If the inspection value is positive then the questionable node is regarded as the normal node. Otherwise the initial detection node will starts the cooperative detection procedure and deals with broadcasting and notifying all one hop neighbor to participate in the decision making. Because the notified mode utilizes broadcasting method and the network traffic is increased. A constrained broadcasting algorithm is used to restrict the notification range within a fixed hop count. A threshold represents the maximum hop count range of cooperative detection messages. Finally global reaction phase is executed to set up a notification system and send warning message to the whole network. There are reaction modes in the global reaction phase.

In the simulation result the notification delivery ratio is from 64.12 (threshold as 1) to 92.93% (threshold as 3) when using different threshold values. When these values are compared with popular AODV routing protocol in MANET the simulation results shows that DCM has higher data delivery ratio and detection rate even if there are various black hole nodes. The control overhead can be reduced due to the distributed design method DCM wastes few overhead inevitably.

5. Backbone Nodes (BBN) Scheme

Vishnu K. and Amos J. Paul addresses the mechanism to detect and remove the black hole and gray hole attack. This solution is able to find the collaborative malicious node which introduce massive packet drop. An idea of the group of backbone nodes used in MANET is originated from [15]. Vishnu K. et al. refers this method to penetrate their system model and also adds a novel scheme to avoid collaborative black and gray attacks.

In this solution the backbone network is established which is constructed from the set of strong backbone nodes (BBNs) over the ad hoc network. These trusted nodes can be allowed to allocate RIP when there is a new arrival of node joining. A node acquires a RIP which means that it is provided with a routing authority. The source node requests the nearest BBN to allot an RIP before transmitting data packet and then sending RREQ to the destination node and the address of RIP. If the source node only receives the destination node RREP then there is no black hole. In this case when the source obtains the RREP packet from RIP it implies that the adversary might be existed in the network. The RIP neighbor nodes change to promiscuous mode as a result of source node sends monitor messages to alert them. This neighborhood not only monitors the packets of designate node but also the suspicious nodes. Furthermore the source nodes send few dummy data packets to test the malicious node. The neighbor nodes monitor the data packets flow and regard it as the black hole if the packet loss rate exceed the normal threshold and notify the source node about a malicious attacker. Then the neighbor node broadcast this alert message to the whole network and adds the malicious nodes to the black hole list. Finally the attacker’s authorization will be deleted and all the nodes will drop the response from nodes in the black list. The proposed

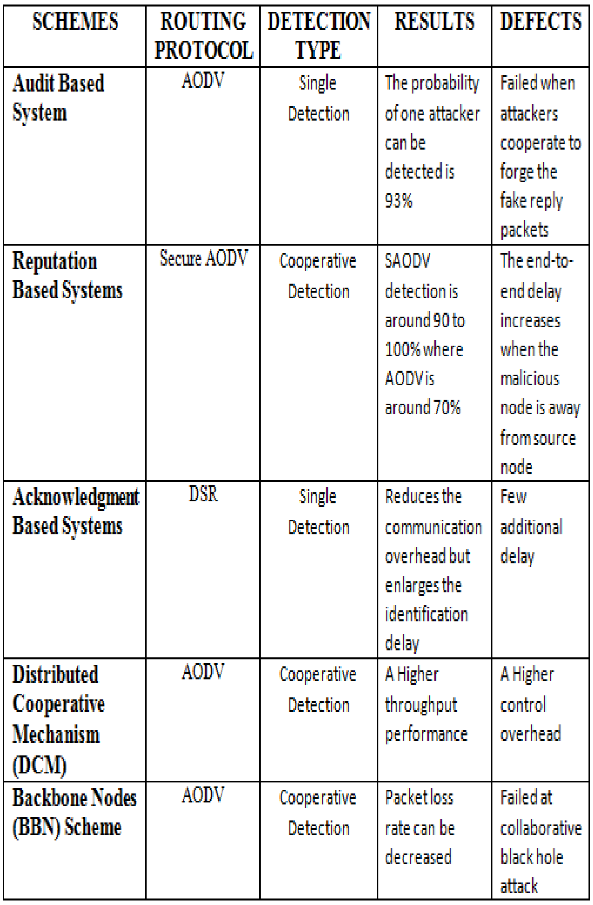
DOI 10.17148/IJARCCE.2017.6297

solution not only detects the black hole but also gray hole attack since its methodology does not utilize the trust based method. However, it is hard to realize that how the enhanced performance because there is no simulation result or experiment.

IV. THE ANALYSIS OF MALICIOUS NODE DETECTION SCHEMES

Feature selection: A systematic effort has been taken to analyse the performance of the traditional and advanced features. Different schemes are utilized for evaluating these features individually. The features with more than 20per cent threshold would be considered as good features. Since single feature is used for classification in this experiment the classification performance would be less than 80 per cent. But this experiment helps to find the good features from each for this malicious node detection. Table 1 shows the different detection schemes.

Table1: Different detection schemes



SCHEMES	ROUTING PROTOCOL	DETECTION TYPE	RESULTS	DEFECTS
Audit Based System	AODV	Single Detection	The probability of one attacker can be detected is 93%	Failed when attackers cooperate to forge the fake reply packets
Reputation Based Systems	Secure AODV	Cooperative Detection	SAODV detection is around 90 to 100% where AODV is around 70%	The end-to-end delay increases when the malicious node is away from source node
Acknowledgment Based Systems	DSR	Single Detection	Reduces the communication overhead but enlarges the identification delay	Few additional delay
Distributed Cooperative Mechanism (DCM)	AODV	Cooperative Detection	A Higher throughput performance	A Higher control overhead
Backbone Nodes (BBN) Scheme	AODV	Cooperative Detection	Packet loss rate can be decreased	Failed at collaborative black hole attack

V. CONCLUSION

Due to the inherent design disadvantages of routing protocol in MANET many researchers has conducted diverse techniques to propose different types of prevention mechanisms for black hole problem. The attackers are able to avoid the detection mechanism no matter what kind of routing detection is used. Some key encryption methods or hash based methods are exploited to solve this problem. The black hole problem is still an active research area. To mitigate the problem of malicious packet dropping, comprehensive selfish node detection and suppression system using three major modules such as watchdog, classifier and diffusion module has been proposed.

REFERENCES

[1] Enrique Hernandez-Orallo et al. “CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes”, IEEE transactions on Mobile Computing, vol. 14, no. 6, June 2015.

[2] S. Buchegger et al., “Self-policing mobile ad hoc networks by reputation systems”. Communications Magazine, IEEE, 43(7):101 – 107, July 2005.

[3] Bansal and M. Baker, “Observation-based cooperation enforcement in ad hoc networks” Stanford University, Tech. Rep., 2003.

[4] Khairu lAzmi Abu Bakar and James Irvine “Contribution Time-based Selfish Nodes Detection Scheme” ISBN: 978-1-902560-24-3 © 2010 PGNet.

[5] M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz”, On the effect of node misbehavior in ad hoc networks. In Proceedings of IEEE International Conference on Communications, ICC’04, pages 3759–3763. IEEE, 2004.

[6] C. K. N. Shailender Gupta and C. Singla, “Impact of selfish node concentration in MANETs”,

[7] C. Toh, D. Kim, S. Oh, and H. Yoo, “The controversy of selfish nodes in ad hoc networks”, In Proceedings of Advanced Communication Technology (ICACT), volume 2, pages 1087 –1092, Feb. 2010.

[8] Y. Yoo, S. Ahn, and D. Agrawal, “A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks”, In Proceedings of IEEEICC, volume 5, pages 3005 – 3009 Vol. 5, may 2005.

[9] S. Marti, T. Giuli, K. Lai, and M. Bakar, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. 6th Annual Int. Conf. on Mobile Computing and Networking (MobiCom’00), August 2000, pp. 255–265.

[10] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in manets,” in IEEE Transactions on Mobile Computing, 2006, pp. 536–550.

[11] Q. He, D. Wu, and P. Khosla, “Sori: A secure and objective reputation based incentive scheme for ad-hoc networks,” in WCNC 2004.

[12] S. Buchegger and J. L. Boudec, “Performance analysis of the confidant protocol: (cooperative of nodes – fairness in dynamic ad hoc networks),” in Proc. IEEE/ACM Workshop on (MobiHoc’02), June 2002, pp. 226–336.

[13] P. Michiardi and R. Molva, “Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” in (CMS’02), September 2002.

[14] K Balakrishnan, J Deng, and P K Varshney, “TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks”, Proc. IEEE Wireless Comm. And Networking, pp. 2137- 2142, 2005

[15] S. Zhong, J. Chen, and Y. Yang, “Sprite: A Simple, Cheat-Proof, Credit- Based System for Mobile Ad- Hoc Networks”, Technical Report, Yale University, July 2002, pp. 1987-1997.

BIOGRAPHY

Tharini N U received a BE degree in Computer Science and Engineering from Vivekananda college of engineering for women in 2015.She currently purses ME in the Department of Computer Science and Engineering at Sri Krishna College of Engineering and Technology, Coimbatore, India. Her research interests include Mobile ad-hoc networks.