IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Investigation of different recent Selfish node detection mechanism for Mobile Adhoc Networks

T.JohnPaulAntony[1], Dr.S.P.Victor[2]

Research Scholar, Bharathiyar University, Coimbatore, India[1]

Dean of Science & Associate Professor in Computer Science, St. Xavier's College, (Autonomous), Palaymkottai, India[2]

Abstract: Mobile Adhoc Network gain much attention because of its uses in various critical areas such as military exercises, Disaster recovery, Mine site operations, etc. As mobile nodes in MANET are autonomous nodes, each mobile node assist their neighbor nodes for packet forwarding towards intended destination. The cooperation among the mobile nodes ensures the reliable communication in MANET. Some mobile nodes refuse to forward the packet from other nodes due to lack of resources or malicious activity. This kind of nodes is called as selfish nodes. The presence of selfish nodes in the route degrades the overall performance of the network. So, this paper aims to review the various selfish node detection mechanisms. The unique features are inspected and the constraints are discussed.

Keywords: Mobile Adhoc network, Selfish nodes, Malicious, Cooperative communication.

I. INTRODUCTION

Mobile Adhoc Network permits the wireless devices to form the network devoid of central authority. This will make the MANET communication very flexible. But, it will make the routing process very difficult. In Mobile Adhoc Networks, each mobile node can communicate with other mobile nodes through wireless channel. The mobile nodes can organize itself without central authority and any special topology. So, the MANET is called as infrastructure less network. The network is launched by radio communication range where each mobile node can act as source node and the relay node. Furthermore, each nodes move freely in the communication environment leads to topology changes in the network. The routing table should be updated as the topology changes during the run time. According to the node speed and mobility model, the topology of the network gets changed.

The infrastructure less property of MANET, the data packets send to the far-away node expected to relay by the other mobile nodes in its range. The data packets are forwarded by the relay nodes until it reach the destination. The routing and data forwarding is done in the network layer. The cooperation among the mobile nodes is vital for the MANET to be operational.

In MANET, relaying the data packets for other nodes is not a direct concern of mobile nodes. So, we cannot expect each mobile node will cooperate with other nodes for forwarding the data packets towards the destination. The path discovery and the data relay will be the significant process of MANET communication. These process carry out by the less trusted nodes will degrade the performance of the MANET communication. Really, the nodes aim to save its resources like battery power and memory space by refuse to forward the data packets for other nodes.

A mobile node will get the advantages from other nodes but decline to serve for other nodes by sharing its resources. This kind of behavior is called as selfishness behavior in the context of MANET communication. The selfishness behavior [8] of the mobile nodes is intentional and unintentional one. The node get the packets from other nodes for forwarding but do not forward the data packets with intention of saving its resources is comes under intentional misbehavior. But due to hardware failure or link failure, a node cannot forward the data packet is come under unintentional misbehavior. The mobile nodes in the MANET have following two behavior models.

- Collaborative Model
- Selfish model

A. Collaborative Model

In this model, a node cooperate with other nodes in a proper manner and perform routing and packet relaying in an efficient manner.

B. Selfish Model

The mobile node refuses to forward the data packets from other nodes in order to save its resources. The selfish node [5] could render inoperative the routing function and packet forwarding.

In this paper, we have analyzed various delegated selfishness detection mechanism proposed in related research articles. The merits and demerits of those schemes are analyzed in this paper.

The rest of the paper is ordered as follows: - Section II reviews the recent selfishness node detection schemes. Section III thrash out our findings and section IV concludes this article.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

II. SECURITY ATTRIBUTES OF MANET

Since MANETs are used for the critical application, MANETs require secure communication between the mobile nodes. The following are the four standard security attributes for MANET.

A. Availability
It denotes the presence of mobile node for communication and should be in the working state. The node should provide the right admission and serviceability to other nodes. Ensuring availability in the MANET communication provides prevention against Denial-of-service attacks.

B. Confidentiality
Confidentiality is the main security aspect of MANET communication. This property ensures that the data transmitted among the mobile node is not accessible or exposé to the unauthorized nodes.

C. Integrity
Integrity in MANET communication means that maintaining and assuring the accuracy of information until it reach the destination. Integrity property ensures that the data cannot be modified in unauthorized manner.

D. Authenticity
This property assuring that the communicating node should be a legitimate node. The contents of a message should be valid.

III. SECURITY CHALLENGES IN MANET

In MANET, each node is an autonomous node, so they can operate like a router to relay the data packets to the destination which is far away from the source node. Furthermore, the mobile nodes in MANET contribute to the same open communication atmosphere; this will give the chance to the misbehaving or attacker nodes [2] to participate in the communication. This is the vital vulnerability of MANET communication. The various security challenges faced by the MANET are summarized as follows:

A. Decentralized Network
Since MANET is a decentralized network, there is no gateway, router, etc. The autonomous mobile nodes itself act as router while forwarding the data to other nodes. The mobile nodes in the MANET have the communication link with the nodes available in its range. This provides the chance to the malicious nodes to participate in the communication.

B. Dynamic Environment
The nodes in the MANET can free to move in the communication environment. Each mobile can join, leave and roam in the communication range of other mobile nodes. If the nodes move into the communication range of other nodes, the communication link will be established. On the other hand, the node move out of communication range of other nodes, the communication link will be failed. So, the topology of the network changes dynamically. The proposed security solution should be adapted with the dynamic nature of MANET.

C. Wireless Communication
The use of wireless channel for the MANET communication leads to collision while send and receive the data packets among the mobile nodes. While Route discovery process and the Broadcast services of MANET causes the flood attack and replay attack.

D. Resource Constraint
The mobile nodes in the MANET communication such as Laptop, Personal Digital Assistant etc., are having limited battery power, storage capacity and processing speed. So, the security solutions to the MANET communication should be lightweight. This may reduce the accuracy and efficiency of security schemes.

E. Cooperative Communication
The cooperation among the mobile nodes [1] is very important feature of MANET communication. The mobile node's intended destination is out of range, it should depend on other nodes for the reliable communication. This will give the chance for attacker nodes to participating in the communication in the unauthentic manner.

IV. DELEGATED SELFISH NODE DETECTION MECHANISM

This section reviews six representative selfishness detection mechanisms and discusses their unique characteristics.

A. CoCoWa
In Collaborative Contact based Watchdog mechanism, the accurate detection of selfish node is consider as the positive event mean while if a node is detected as a non-selfish node, the event is consider as a negative event.

In the CoCoWa model, each mobile node is preloaded with watchdog [15] mechanism. Each mobile node continuously monitors the traffic inflow and outflow of the mobile nodes. If any node discovers the selfishness behavior in its neighbors, immediately it will spread the information about selfish nodes. So, the information regarding selfish nodes i s collocated [4] in a fast manner. The link between the nodes in MANET changes frequently as all the nodes are moving.

The nodes can overhear the communication of the nodes which are present inside its communication range. So, sometimes, they cannot get the accurate information about other nodes to decide whether they are behaving selfishly or not.

In CoCoWa mechanism, the information is update frequently based on the direct estimation as well as indirect information about selfish nodes from other nodes.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

B. RTBD

In [14], The Record and Trust Based Detection method is proposed to discover the selfish nodes proficiently in MANET. The use of trust in the process of discovering the selfish nodes will speed up the detection process. RTBD examines the discovery of selfish nodes on routing [7] and packet dropping. RTBD method comprises of packet dropping detection scheme and selfish node mitigation scheme. The trust report is generated by each mobile node which reports the prior communication behavior of its neighbor nodes. This report is used to detect that the selfish nodes has dropped the packets. Each node congregates the trust report to detect false report and by which it will find out which node has dropped the packet. In this context, selfish node may share the false report to conceal its packet dropping behavior from being detected.

The trustworthiness of a node is assessed with respect to the prior performance of the node. Each node evaluate the trust of its neighbors, it will build the trust model. RTBD provides the powerful mechanism to detect the abnormal node behavior. Once the node is predicted as the selfish node, its neighbor nodes use this prediction to decline the packet for forwarding from selfish nodes.

C. CORE

In [6], the authors distinguish the selfish nodes from the malicious nodes. The selfish node use their resources for their own communication alone while not cooperate with other nodes in packet forwarding towards the destination. The selfish nodes expect other nodes to cooperate with them. The malicious nodes affect its neighbor nodes by making network unavailable. The authors proposed a novel technique Collaborative Reputation mechanism (CORE) to insist the cooperation among the mobile nodes in MANET. Three types of reputation values are used by the CORE such as,

- Indirect Reputation
- Subjective Reputation
- Functional Reputation

Subjective Reputation is the reputation value determined based on the local observation of a node with respect to other mobiles nodes in the network. Indirect reputation is the reputation value get from other nodes in the network. Functional reputation [12]is computed by merging the subjective reputation and the indirect reputation by using weighted combining formula to obtain the final reputation value in order to select a node to forward the packet. The functional reputation values are combined together to determine the global reputation value. Subjective reputation values get updated with respect to the misbehavior identification by watchdog mechanism [3]. Indirect reputation values get updated with respect to the reply message. The reply message contains the information about the truthful behavior identified in each operation. If the reputation of a mobile node is negative, the request from that mobile node is denied by all other remaining nodes in the network. The CORE failed to consider the second chance method.

D. AMD

Audit based misbehavior detection (AMD) segregate [10] the black hole and grayhole attackers. Black hole attacker continuously drops the data packet mean while grayhole attacker selectively drops the data packet. AMD consist of following modules:

- Reputation Management
- Trust worthy Route discovery
- Identification of misbehaving nodes

AMD assesses the performance of a node in a Per-packet basis. AMD does not use the energy exclusive overhearing techniques or rigorous acknowledgement schemes. It will reduce the selfishness behavior of nodes in the network. AMD can avoid the misbehaving nodes in the communication even maximum number of nodes become selfish nodes.

E. Sprite

In [11], the authors have proposed Sprite (Simple, Cheat-proof, and credit based system) for inspiring cooperation between the mobile nodes in the Mobile Adhoc Networks. Sprite offers incentive to mobile nodes for full cooperation and report events truthfully. In Sprite, each node has a certificate issued by the Scalable certificate authority.

If the intended destination is out of range, the source mobile node depends on other nodes for the successful delivery of the message. The source node will lose its credit [9] because of the nodes support source node to forward the data successfully to the destination incur a charge for relay the message. So, if a node forwards the data packets for other node, it will gain the credit. This gained credit value is used for its own communication. To save the resources of resource constrained mobile nodes, Sprite uses the tiny receipt as a report as an alternative of having whole message as a report. The receipts are resulting from the content of the messages.

V. SUMMARY REPORT OF VARIOUS SELFISH NODE DETECTION MECHANISM

The summary report for the various selfish node detection mechanisms are presented by Table I

TABLE I: SUMMARY REPORT

Protocol	Technique Used	Merits	Demerits
CoCoWa	Mutual Neighbor based watchdog mechanism	• Detects the selfish nodes in a quick manner. • High Accuracy.	The information about selfish nodes are flooded if a node detect the new neighbor node causes overhead sometime.
RTBD	Trustworthiness of a node is used to detect the selfish nodes	• Detection time of selfish nodes is reduced. • Overall overhead is low.	Do not consider the node compromisation attack by selfish node
CORE	Indirect, Subjective and functional reputation values are used	• Truthful behavior of mobile nodes is identified based on the reputation values. • Neglect the selfish nodes thoroughly in the communication.	Second chance method is not considered
AMD	Asses the performance of a node in a per packet basis	• Reduce the selfishness behavior of nodes in the network. • Avoid the misbehaving nodes in the communication even maximum number of nodes become selfish nodes.	Leads to overhead because of analyzing performance of a node
Sprite	Provides incentive to mobile nodes to cooperate	• Overhead is small. • Mobile nodes can cooperate and forward each other's message.	No punishment scheme is there for selfish nodes.

DOI 10.17148/IJARCCE.2016.5532

VI. CONCLUSION

This paper surveyed various selfish node detection techniques. The mechanism used in the technique and constraints are discussed. This paper presents the importance of detecting selfish nodes in MANET. The delegated selfish node detection mechanism way out the problem of selfishness behavior but consumes much resources. From this survey, we found that the CoCoWa detects the selfish nodes with high accuracy among other existing methods. While reviewing the various recent selfishness detection techniques, we discover some points to implement in future to increase the performance of MANET communication such as Altruistic path planning methodologies for MANET.

REFERENCES

[1]. S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks" arXiv:cs.NI/0307012, 2003.
[2]. J. R. Douceur, "The sybil attack," in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., 2002, pp. 251–260.
[3]. E. Hern_andez-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni, "Improving selfish node detection in MANETs using a collaborative watchdog," IEEE Comm. Lett., vol. 16, no. 5, pp. 642–645, May 2012.
[4]. E. Hern_andez-Orallo, M. D. Serrat Olmos, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Evaluation of collaborative selfish node detection in MANETS and DTNs," in Proc. 15th ACM Int. Conf. Modeling, Anal. Simul. Wireless Mobile Syst., New York, NY, USA, 2012, pp. 159–166.
[5]. F. Kargl, A. Klenk, S. Schlott, and M. Weber, "Advanced detection of selfish or malicious nodes in ad hoc networks," in Proc. 1st Eur.Conf. Security Ad-Hoc Sens. Netw., 2004, pp. 152–165.
[6]. P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proc. 6th Joint Working Conf. Commun. Multimedia Secur., 2002, pp. 107–121.
[7]. K. Paul and D. Westhoff, "Context aware detection of selfish nodes in DSR based ad-hoc networks," in Proc. IEEE Global Telecommun. Conf., 2002, pp. 178–182.
[8]. C. K. N. Shailender Gupta and C. Singla, "Impact of selfish node concentration in MANETs," Int. J. Wireless Mobile Netw., vol. 3, no. 2, pp. 29–37, Apr. 2011.
[9]. Y. Yoo, S. Ahn, and D. Agrawal, "A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks," in Proc. IEEE Int. Conf. Commun., May 2005, vol. 5, pp. 3005–3009.
[10]. Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," IEEE Trans. Mobile Comput., vol. PP, no. 99, 2012, http://doi.ieeecomputersociety. org/10.1109/TMC.2012.257.
[11]. S. Zhong, J. Chen, and Y. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in Proc. IEEE Conf. Comput. Commun., Mar. 2003, vol. 3, pp. 1987–1997.
[12]. M. Sreedevi, "A Reputation Based Scheme to Prevent Routing Misbehavior in MANETs", International Journal of Computer Science and Information Technologies, Vol. 3 (2), 3526-3529, 2012.
[13]. Enrique Hern_andez-Orallo, "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes", IEEE Transactions on Mobile computing, vol. 14, no. 6, June 2015.
[14]. Senthilkumar Subramaniyan, William Johnson and, Karthikeyan Subramaniyan, "A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique", EURASIP Journal on Wireless Communications and Networking2014.
[15]. Reshma Lill Mathew, P. Petchimuthu, "Detecting Selfish Nodes in MANETs Using Collaborative Watchdogs", IJARCSSE 2013.

DOI 10.17148/IJARCCE.2016.5532