IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Comparative Analysis of Prevention and Detection Policies for Selfish Behaviour in MANET

Ms. Lilu Odedra[1], Prof. Ashish Revar[2], Prof. Munindra H. Lunagaria[3]

PG Scholar, Department of Computer Engineering, Faculty of PG Studies-MEFGI, Rajkot, India[1]

Assistant Professor, Department of Computer Engineering, Faculty of PG Studies-MEFGI, Rajkot, India[2, 3]

Abstract: Mobile Ad-hoc Network (MANET) is infrastructure less and central object less network in which the mobile nodes can communicate using wireless links. Due to this, Network is vulnerable to many attacks. This paper focuses on selfish behaviour and different countermeasures available. Nodes may deny participating in the routing process for its own benefits like to save battery, storage space, bandwidth etc. Various policies like token based, credit based, reputation based, trust based etc. are used to detect and prevent selfishness.

Keywords: Network Security, MANET, Selfish attack, countermeasures, wireless security.

I. INTRODUCTION

MANET is self-organized network which has no infrastructure so, any node is free to join and leave network. This paper focuses on the selfish attack in which node will act as selfish and do not forward packets of other node to save its network resources like energy, storage space, CPU cycles, network bandwidth etc. just for its own data transmission. The selfish nodes do not forward the packets of the other nodes which may degrade network performance.

The rest of the paper has been organized in following sections (II) Types of the selfish behaviours (III) Existing techniques (IV) Conclusion.

II. TYPE OF SELFISH BEHAVIOURS

The various selfish behaviors are performed by the nodes by not forwarding data of other nodes, which all are described as below:

1. Forwarding Node Selfish Behavior

The selfish node does not forward the packets of other nodes to save its resources. As shown in the analysis by Abdelaziz Babakhouya et al. [1] Selfish node may decide to do not consume their resource in forwarding data packets for other. Based on author's simulation packet data fraction is same as the high and low density of nodes and percentage of selfish node increase the end-to-end delay is increased.

2. MAC layer Selfish Behaviors

The selfish node misuses the MAC protocol to gain more network resources than well behaved node through that it obtain large portion of channel and capacity to improve its throughput. Lei Guang et al. [2] observe that Selfish node choose smaller back off interval, thereby increasing its accessing channel capacity and hence reduce the throughput share received by well-behaved nodes.

3. Set TTL field to zero misbehavior

Hyun Jin Kim et al. [3] State that selfish nodes drop routing packets or forward with at Time to live (TTL) of 0 so that no path can be established. They may artificially increase hop count so other nodes mostly don't prefer that path.

4. Disobey the Protocol Specification rules to get higher throughput

R. Gunasekaran et al. [4] stated that nodes can deviate from the protocol specification in order to obtain a given goal, at expense of honest participants and disobey the rules for access the wireless channel in order to obtain higher throughput than other nodes it is by back off manipulation, shorter DIFS and oversize NAV.

5. Network card on/off selfish behaviors

Hemang Kothari et al. [5] stated that in network card on/off selfish behavior the node refusing to forward any control or data packets for others by Turn off the power of network card or by Turn off the communication function when they do not need to communicate. Authors stated that this behavior saves more energy than the other selfish behaviors.

6. Partial Dropping Misbehavior

Djamel DJENOURI et al. [6] shows that in watchdog mechanism node can't be detected as wrong by dropping packets at lower rate than watchdog's configured minimum misbehavior threshold.

7. False Accusation misbehavior

Djamel DJENOURI et al. [6] Shows that the node may falsely accuse the legitimated node by adjusting the transmission power. The selfish node keeps its transmission power more toward source node and less toward adjacent node and do not forward packets to its adjacent node so source can't hear transmission of next node of selfish node and selfish node falsely accused a legitimated node as selfish.

8. Link Breakage Selfish Behavior

In Wei Yu and K.J. Ray Liu [7] selfish node silent about the

link breakage in path and do not inform to source, so it wastes other node's energy and put down all of nodes into the starvation.

III.EXISTING TECHNIQUES

1. DREAM-Detection & Reaction to Timeout MAC layer Misbehaviour

Lei Guang, Chadi Assi et al. [8] Proposed mechanism that identify the malicious nodes using a set of monitoring and reaction procedures. It use two stage reaction, first stage is for reaction and second stage is for punishment that can improve the network performance. This system gives the high accuracy in identifying misbehaved nodes. First reaction system is very effective to mitigate misbehaving effect and improve network performance.

2. LOTTO-low overhead truthful protocol for MANET

Yongwei et al [9] proposed a scheme where a node may use different cost to send packets to different neighbors. The network topology information is collected by only one RREQ message and from that least cost path from the source node to the destination node can be found. By applying VCG mechanism, LOTTO assure that node will get enough payment and have no incentive to cheat over their cost. It reduces overhead from O (n^3) to O (n^2) compared with VCG mechanism.

3. Identification of malicious nodes in an AODV pure ad hoc network through guard nodes

Imran Raza et al. [10] proposed a guard node based scheme to identify malicious nodes in AODV protocol. In this each node calculates trust level of its neighboring nodes for route selection. Trust calculation process based on opinions of other nodes .The identification process of malicious nodes is dynamic because trust level of a node is increased or decreased. If neighboring node has trust level lower than a predefined threshold, it is accusing as the malicious and does not consider in route selection.

4. A Modular Solution for Isolation

Djamel Djenouri et al. [11] proposed a solution to monitor, detect and safely isolate misbehaving nodes. The process includes five modules 1) monitor control the forwarding of packets, 2) Detector is to detect misbehaving of monitored nodes, 3) isolator is used to isolate misbehaving nodes detected by detector, 4) investigator, which investigates accusations before testifying when the node has not enough experience with accused, 5) witness module that responds to witness request of the isolator.

5. Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks

Abdurrahman Baadache et al. [12] Proposed mechanism to verify the correct forwarding of packets by the intermediate nodes. The merkle tree principle has been used for implementation of this approach. All intermediate nodes need to acknowledge the reception of the packet. Using this source node construct a merkel tree and compares the value of tree root with previously calculated values. If both values are equal then end-to-end path is packet dropper free.

6. Fully Selfish Node Detection, Deletion and Secure Replica Allocation over MANET

N. Muthumalati et al. [13] Proposed an approach which stated that Selfish node may not share its own memory space to store replica for the benefits of other nodes. Every node calculates credit risk information on other connected nodes individually to measure the degree of selfishness. Selfish allocation technique reduces communication cost and secure hill cipher algorithm to provide security in replica data.

7. SENSE: A Collaborative selfish node detection and incentive mechanism for opportunistic networks

Radu-Ioan Ciobanu et al. [14] proposed an approach SENSE that provide the selfish node detection by using community based and context based information of node. By using intensive mechanism it will appreciate the node to participate in the network. Use the altruism value to get the selfishness of node. It uses the home-cell community model for mobility model.

8. RTDB: Record and Trust Based Detection Technique

Senthilkumar Subramanian et al. [15] proposed a technique in which every node maintains global trust state for all nodes which is recorded in trust table. The selfish nodes are detected based on their trust value and predefined threshold for selfishness, their neighbours can use this information to avoid working with them, either for data forwarding, data aggregation, or any other cooperative function.

9. Reputation based selfishness prevention techniques for mobile ad-hoc networks.

Alberto Rodriguez-Mayol et al. [16] Proposed a three detection techniques that improve the ability of selfishness prevention protocol to detect selfish nodes and to increase the number of valid routes. That three techniques are RAM (reset activity mode), WM (warming mode) & RFM (reset failure mode).The study of proposed techniques are implemented with TEAM & Marti's protocol.

10. TBUT (Token-based umpiring technique)

Jebakumar Mohan Singh Pappaji Josh Kumar et al. [17] proposed a unified approach for detecting and elimination selfish nodes in MANETs using TBUT.it is the token-based umpiring technique where every node needs a token to participate in the network and the neighboring nodes acts as an umpire. Umpire nodes will monitor the behavior of the nodes and detect if any node is misbehaving. It is very efficient with reduced detection time and less overhead.

IV.CONCLUSION

This paper discusses various types of selfish behaviors and existing techniques for detection and prevention of such attacks. Few of techniques improve the network performance by isolating selfish nodes or encouraging good bodes for their behavior. In any method, there is drawback of false accusation, high overhead, resource usage and higher processing. It is concluded that MANET

requires a mechanism against selfish behavior which overcomes all these issues.

REFERENCES

[1] Babakhouya, Abdelaziz, Yacine Challal, and Abdelmadjid Bouabdallah. "A simulation analysis of routing misbehaviour in mobile ad hoc networks." In Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST'08. The Second International Conference on, pp. 592-597. IEEE, 2008.

[2] Guang, Lei, and Chadi Assi. "Mitigating smart selfish MAC layer misbehavior in ad hoc networks." In Wireless and Mobile Computing, Networking and Communications, 2006.(WiMob'2006). IEEE International Conference on, pp. 116-123. IEEE, 2006.

[3] Kim, Hyun Jin, and Jon M. Peha. "Detecting selfish behavior in a cooperative commons." In New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on, pp. 1-12. IEEE, 2008.

[4] Gunasekaran, R., V. Rhymend Uthariaraj, R. Sudharsan, S. Sujitha Priyadarshini, and U. Yamini. "Detection and prevention of selfish and misbehaving nodes at MAC layer in mobile ad hoc networks." In Electrical and Computer Engineering, 2008. CCECE 2008. Canadian Conference on, pp. 001945-001948. IEEE, 2008.

[5] Kothari, Hemang, and Manish Chaturvedi. "Effect of Selfish Behavior on Power Consumption in Mobile Ad Hoc Network." Proceedings of the Asia-Pacific Advanced Network 32 (2011): 91-100.

[6] Djenouri, Djamel, and Nadjib Badache. Two hops ack: A new approach for selfish nodes detection in mobile ad hoc networks. Technical report LSI-TRO704, University of Scinece and technology houari boumediene, Algiers, Algeria, 2003.

[7] Yu, Wei, and K. J. Liu. "Attack-resistant cooperation stimulation in autonomous ad hoc networks." Selected Areas in Communications, IEEE Journal on 23, no. 12 (2005): 2260-2271.

[8] Guang, Lei, Chadi Assi, and Yinghua Ye. "DREAM: A system for detection and reaction against MAC layer misbehavior in ad hoc networks." Computer communications 30, no. 8 (2007): 1841-1853.

[9] Wang, Yongwei, and Mukesh Singhal. "On improving the efficiency of truthful routing in MANETs with selfish nodes." Pervasive and Mobile Computing 3, no. 5 (2007): 537-559.

[10] Raza, Imran, and Syed Asad Hussain. "Identification of malicious nodes in an AODV pure ad hoc network through guard nodes." Computer Communications 31, no. 9 (2008): 1796-1802.

[11] Djenouri, Djamel, and Nadjib Badache. "On eliminating packet droppers in MANET: A modular solution." Ad Hoc Networks 7, no. 6 (2009): 1243-1258.

[12] Baadache, Abderrahmane, and Ali Belmehdi. "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks." Journal of Network and Computer Applications 35, no. 3 (2012): 1130-1139.

[13] Muthumalathi, N., and M. Mohamed Raseen. "Fully selfish node detection, deletion and secure replica allocation over MANET." In Current Trends in Engineering and Technology (ICCTET), 2013 International Conference on, pp. 413-415. IEEE, 2013.

[14] Ciobanu, Radu-Ioan, Ciprian Dobre, Mihai Dascălu, Ştefan Trăuşan-Matu, and Valentin Cristea. "SENSE: A collaborative selfish node detection and incentive mechanism for opportunistic networks." Journal of Network and Computer Applications 41 (2014): 240-249.

[15] Subramaniyan, Senthilkumar, 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 Networking 2014, no. 1 (2014): 1-10.

[16] Rodriguez-Mayol, Alberto, and Javier Gozalvez. "Reputation based selfishness prevention techniques for mobile ad-hoc networks." Telecommunication Systems 57, no. 2 (2014): 181-195.

[17] Kumar, Jebakumar MSP Josh, Ayyaswamy Kathirvel, Namaskaram Kirubakaran, Perumal Sivaraman, and Muthusamy Subramaniam. "A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT." EURASIP Journal on Wireless Communications and Networking 2015, no. 1 (2015): 143.