International Journal of Research in Advent Technology, Vol.3, No.8, August 2015
E-ISSN: 2321-9637

Survey on Selfish Node Detection System in MANETs

Mangesh M. Ghonge[1], Dr. P. M. Jawandhiya[2]
Assistant Professor[1], Professor & Principal[2]
JCOET, Yavatmal[1]
PLIT & MS, Buldhana[2]
mangesh.cse@gmail.com[1], pmjawandhiya@rediffmail.com [2]

Abstract—Combine effort of nodes in Mobile Ad hoc Network makes it more powerful. But supporting a MANET is a cost-intensive activity for a mobile node. Finding routes and forwarding packets consumes bandwidth and energy. One such routing misbehavior is that some nodes may be act as selfish by participating in route discovery and maintenance process, but deny to forward the packet. Such nodes routing misbehavior reduces the packet delivery ratio and wastes system resources such as power and bandwidth. MANETs lack a centralized monitoring and management point, making it a challenging task to detect such misbehaving nodes effectively. This paper surveys existing & latest developments in selfish node detection system in MANETs. Finally, we conclude this survey paper with some future work.

Index Terms—MANETs, selfish, node, misbehavior, detection;

1. INTRODUCTION

Mobile Wireless Ad hoc Network (MANET) is a group of autonomous mobile nodes or devices connected through wireless links without the support of a communications infrastructure. The topology of the network changes dynamically as nodes move and the nodes reorganize themselves to enable communications with nodes beyond their immediate wireless communications range by relaying messages for one another [1], i.e. multihop.

MANET relies on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET becomes. But supporting a MANET is a cost-intensive activity for a mobile node. Detecting routes and forwarding packets consumes network-bandwidth, local CPU time, memory, and energy. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data [2]. In recent years, many possible applications of ad hoc networks are discussed, such as in sensor networks, conference meetings and extending of the range of base stations through the use of ad hoc networks. In these applications, the nodes do not always belong to one owner or share a common objective, as a result nodes may not be willing to route packets for other nodes for various reasons. These reasons can include commercial benefits or it may want to preserve its own battery life [3]. Due to the nature of the wireless medium, malicious nodes, which may not belong to any organisation, can disrupt the operations of ad hoc networks by injecting wrong routing information or injecting forged data packets. Moreover, viruses can disrupt the operations of networks by modifying the behavior of routing protocols or creating denial-of-service attacks by sending large number of forged routing or data packets into the network [4].

Security is a key concern in MANETs because their nodes are generally more susceptible to various threats than those in traditional wired networks. Current schemes of detecting node selfishness in MANET are mostly centered on using audit, incentives, reputation, price or acknowledgement based mechanisms to achieve the desired effect of nodes cooperation. Selfishness in its worse form involves a deliberate intent by a node or group of nodes to disrupt the operation of the network for its own objectives. Such nodes are termed malicious and dealing with them would involve the areas of providing security in MANETs [5].

2. MANETS: FEATURES, CHARACTERISTICS AND RESEARCH ISSUES

A. MANETs Features

1) Autonomous Terminal

In Ad hoc Network, each mobile terminal is an autonomous node, which may function as both a host and a router. In other, since there is no background network words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in Ad hoc Network.

2) Distributed Operation

For the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a Ad hoc Network should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

3) Multihop Routing

Basic types of ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop Ad hoc Network is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes

4) Light-weight Terminal

In most cases, the Ad hoc Network nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

B. MANETs Characteristics

Ad hoc Networks are new paradigm of networks, offering unrestricted mobility without any underlying infrastructure. Basically, ad hoc network is a collection of nodes communicating with each other by forming a multi-hop network. Following are the characteristics of a Ad hoc Network [26, 28]:

1) Dynamic Topologies

Nodes are free to move arbitrarily. The network topology may change randomly and have no restriction on their distance from other nodes. As a result of this random movement, the whole topology is changing in an unpredictable manner, which in turn gives rise to both directional as well as unidirectional links between the nodes.

2) Energy Constrained Operation

Almost all the nodes in an ad hoc network rely on batteries or other exhaustive means for their energy. The battery depletes due to extra work performed by the node in order to survive the network. Therefore, energy conservation is an important design optimization criterion.

3) Bandwidth Constraint

Wireless links have significantly lower capacity than infrastructures networks. Throughput of wireless communication is much less because of the effect of the multiple access, fading, noise, interference conditions. As a result of this, congestion becomes a bottleneck in bandwidth utilization.

4) Limited Physical Security

Ad hoc Networks are generally more prone to physical security threats than wireless networks because the ad hoc network is a distributed system and all the security threats relevant to such a system are pretty much present, as a result, there is an increased possibility of eavesdropping, spoofing, masquerading [ ], and denial-of- service type attacks.

C. MANETs Research Issues

There are many research problems that must be solved to support the implementation of MANETs [5]. Solutions to these problems should be compromise of all three components prevention, detection and reaction. Following performance related issues are to be handled in MANETs:

1) Degraded performance in larger networks
- Need of techniques to handle transmission impediments such as path loss, fading, interference and blockage.
- The path discovery causes considerable delays in larger networks.
- The overhead caused by the exchange of control signals also contributes to the slow response and decreased data rates.

2) Routing algorithms
- The routing algorithms, currently used for wired networks, are least likely useful in MANETs due to the environmental variables.
- New algorithms have to be introduced for use in this new type of networks.

3) Mobility induced route changes
- The network topology in an ad hoc wireless network is highly dynamic. Techniques are needed to effectively adapt to these changes.
- An on-going session suffers frequent path breaks due to the movement of nodes. This situation often leads to frequent route changes.

4) Mobility Management Methods
- The functionality of mobile nodes and networks, wireless communication allows changing their position based on the predefined trajectories, orbits and randomly selected routes.
- The possibility to control the movement of mobile node allows more effective prediction and scheduling of network sources for

individual stations, such as handover optimization in MANETs.

5) *Limited wireless transmission bandwidth*
   - In wireless networks the radio band will be limited and hence data rates it can offer are much lesser than what a wired network can offer.
   - It is required that the routing protocols in wireless networks use the bandwidth always in an optimal manner by keeping the overhead as low as possible.
6) *Cross layered architecture*
   - It is proposed that cross layered design is suitable for the MNETs rather than the TCP-IP layered architecture.
   - The cross layered approaches are generally application specific. The approach should be generic to support diverse networks to be interconnected efficiently and should consider the totality of the design while considering the long term architectural value.
7) *Security issues*
   - Due to its broadcast nature, data transmitted by a node is received by all the nodes within its direct transmission range. So an attacker can easily snoop the data being transmitted in the network. Thus there is a requirement of confidentiality of data.
8) *Battery constraints*
   - Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device. These constraints affect the route maintenance due to reduced performance and loss of paths. This should be considered at the time of path selection.
9) *Group Membership Control*
   - Secure admission of members to a group while tolerating adversaries from both outside inside.
   - Use of distributed cryptography in MANETs.
10) *Key Distribution*
   - Combining key pre-distribution with secret sharing to achieve key distribution in MANETs.
   - Need a secure and efficient key-distribution mechanism allowing simple key establishment for large-scale sensor networks.

3. LITERATURE REVIEW

Previously proposed methods for detecting node selfish or malicious misbehaviors can be classified into
(a) Audit based system
(b) Credit based systems
(c) Reputation based systems
(d) Acknowledgment based systems
(e) Collaborative based system

Audit Based System: Audit-based system that 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 effectively and efficiently isolates both continuous and selective packet droppers. The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioral audits. William Kozma Jr.and Loukas Lazos [7] proposed a novel misbehavior identification scheme called REAct that provides resource-eficient account ability for node misbehavior. REAct identifies misbehaving nodes based on a series of random audits triggered upon a performance drop.

Credit Based Systems: Credit-based systems are designed to provide incentives for forwarding packets. Buttyan and Hubaux [8] proposed a system in which nodes accumulate credit for every packet they forward, and spend their credit to transmit their own packets. To ensure correctness, the credit counter is implemented in tamper-proof hardware. Zhong et al. [33] proposed Sprite, in which nodes collect *receipts* for the packets they forward to other nodes. When the node has a high-speed link to a Credit Clearance Service (CCS), it uploads its receipts and obtains credit. Crowcroft et al. [9] proposed a scheme that adjusts the credit reward to traffic and congestion conditions. While credit-based systems motivate selfish nodes to cooperate, they provide no incentive to malicious nodes. Such nodes have no intend to collect credit for forwarding their own traffic. Moreover, credit-based systems do not identify misbehaving nodes, thus allowing them to remain within the network indefinitely.

Reputation Based Systems: Reputation-based systems use ratings for evaluating the trustworthiness of nodes in forwarding traffic. These ratings are dynamically adjusted based on the nodes' observed behavior. In the context of ad hoc networks, Ganeriwal and Srivastava [10] developed a Bayesian model to map binary ratings to reputation metrics, using a beta probability density function. Jøsang and Ismail [11] proposed a similar ranking system that utilized direct feedback received from onehop neighbors. Michiardi and Molva [12] proposed the CORE mechanism for computing, distributing, and updating reputation values composed from disparate sources of information. Reputation-based systems use neighboring monitoring techniques to evaluate the behavior of nodes. Marti et al. [13] proposed a scheme which relies on two modules, the

watchdog and the *pathrater*. The watchdog module is responsible for overhearing the transmission of a successor node, thus verifying the successful packet forwarding to the next hop. The pathrater module uses the accusations generated by the watchdog module to select paths free of misbehaving nodes. Buchegger and Le Boudec [14] proposed a scheme called CONFIDANT, which extends the watchdog module to all one-hop neighbors that can monitor nearby transmissions (not just the predecessor node). When misbehavior is detected, monitoring nodes broadcast alarm messages in order to notify their peers of the detected misbehavior and adjust the corresponding reputation values. Similar monitoring techniques have also been used in. Transmission overhearing becomes highly complex in multichannel networks or when nodes are equipped with directional antennas. Neighboring nodes may be engaged in parallel transmissions in orthogonal channels or different sectors thus being unable to monitor their peers. Moreover, operating radios in promiscuous mode for the purpose of overhearing requires up to 0.5 times the amount of energy for transmitting a message [34].

Acknowledgment Based Systems: Acknowledgment-based systems rely on the reception of acknowledgments to verify that a message was forwarded to the next hop. Balakrishnan et al. [16] proposed a scheme called TWOACK, where nodes explicitly send 2-hop acknowledgment messages along the reverse path, verifying that the intermediate node faithfully forwarded packets. Packets that have not yet been acknowledged remain in a cache until they expire. A value is assigned to the quantity/frequency of un-verified packets to determine misbehavior. Liu et al. [17] improved on TWOACK by proposing 2ACK. Similar to TWOACK, nodes explicitly send 2-hop acknowledgments to verify cooperation. Xue and Nahrstedt [18] proposed the Best-effort Fault-Tolerant Routing scheme, which relies on endto- end acknowledgment messages to monitor packet delivery ratio and select routing paths which avoid misbehaving nodes. Awerbuch et al. [19] proposed an on-demand secure routing protocol (ODSBR) that identifies misbehaving links. The source probes intermediate nodes to acknowledge each packet and performs a binary search to identify the link where packets are dropped. ACK-based systems also incur a high communication and energy overhead for behavioral monitoring. For each packet transmitted by the source, several acknowledgements must be transmitted and received over several hops. Moreover, they cannot detect attacks of selective nature over encrypted end-to-end flows.

Collaborative Based system: Enrique Hern_andez-Orallo et al. [33] proposed Collaborative Contact-based Watchdog (CoCoWa) as a new scheme for detecting selfish nodes that combines local watchdog detections and the dissemination of this information on the network. If one node has previously detected a selfish node it can transmit this information to other nodes when a contact occurs. This way, nodes have second hand information about the selfish nodes in the network.

4. CONCLUSION AND FUTURE RESEARCH

To conclude, we first present a brief summary of the whole article. Finding routes and forwarding packets consumes bandwidth and energy. Selfish nodes participate in route discovery and maintenance process and deny to forward the packet. Such nodes routing misbehavior reduces the packet delivery ratio and wastes system resources such as power and bandwidth. MANETs lack a centralized monitoring and management point, making it a challenging task to detect such misbehaving nodes effectively. In this paper, we have provided a literature survey of recent developments in selfish node detection system.
During the survey, we also find some points that can be further explored in the future, such as to find Social Selfishness Aware Routing solutions and detect selfish node in the MANET.

REFERENCES

[1] C. S. R. Murthy and B. S. Manoj, “Ad Hoc Wireless Networks: Architectures and Protocols”, Prentice Hall, 2004.
[2] P. Papadimitratos and Z. J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," presented at Symposium on Applications and the Internet Workshops, Orlando, FL, USA, 2003.
[3] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, 2004.
[4] P. Yau and C. J. Mitchell, "Security vulnerabilities in ad hoc networks," presented at The Seventh International Symposium on Communication Theory and Applications,, Ambleside, Lake District, UK, 2003.
[5] Sudha Singh, S.C. Dutta, and D.K. Singh, “A study on Recent Research Trends in MANET” International Journal of Research and Reviews in Computer Science (IJRRCS)., Vol. 3, no. 3, pp. 1654–1658,. June 2012.
[6] Yu Zhang, Loukas Lazos, William Kozma, "AMD: Audit-based Misbehavior Detection in Wireless

Ad Hoc Networks," IEEE Transactions on Mobile Computing, 06 Sept. 2013.

[7] William Kozma Jr., Loukas Lazos. "REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits", 10th IEEE Symposium on Computers and Communications, 27-30 June 2005.

[8] L. Buttyan and J.-P. Hubaux, "Stimulating Cooperation in Self-organizing Mobile Ad hoc Networks", Mobile Net. and Applications, 8(5):579–592, 2003.

[9] J. Crowcroft, R. Gibbens, F. Kelly, and S. O¨ string. Modelling incentives for collaboration in mobile ad hoc networks. In Proc. of WiOpt, 2003.

[10] S. Buchegger and J.-Y. L. Boudec. Self-policing mobile ad-hoc networks by reputation systems. IEEE Comm. Magazine, pages 101–107, 2005.

[11] S. Ganeriwal, L. Balzano, and M. Srivastava. Reputation-based framework for high integrity sensor networks. ACM Transctions on Sensor Networks, 4(3):1–37, 2008.

[12] Q. He, D. Wu, and P. Khosla. SORI: A secure and objective reputation-based incentive scheme for ad hoc networks. In Proc. of WCNC, 2004.

[13] A. Jøsang and R. Ismail. The beta reputation system. In Proc. of the 15th Bled Electronic Commerce Conference, pages 324–337, 2002.

[14] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proc. of MobiCom, pages 255–265, 2000.

[15] S. Soltanali, S. Pirahesh, S. Niksefat, and M. Sabaei. An Efficient Schemeto Motivate Cooperation in Mobile Ad hoc Networks. In Proc. of ICNS, pages 92–98, 2007.

[16] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM Transactions on Information System Security, 10(4):11–35, 2008.

[17] K. Balakrishnan, J. Deng, and P. K. Varshney. Twoack: Preventing selfishness in mobile ad hoc networks. In Proc. of WCNC, 2005.

[18] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan. An acknowledgment based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5):536–550, 2007.

[19] P. Michiardi and R. Molva. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proc. of CMS, pages 107–121, 2002.

[20] V.-N. Padmanabhan and D. R. Simon, "Secure trace route to detect faulty or malicious routing", SIGCOMM CCR, 33(1), 2003.

[21] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad-hoc routing service in adversarial environments", Wireless Personal Communications, Special Issue on Security for Next Generation Communications, 29(3-4):367–388, 2004.

[22] Sowmiya Hariharan, Jothi Precia, Suriyakala.C.D, Prayla Shyry, "A Novel Approach for Detection of Routes with Misbehaving Nodes in MANETs", ACEEE Int. J. on Network Security, Vol. 02, No. 01, Jan 2011.

[23] 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.

[24] Aishwarya Anand S Ukey, Meenu Chawla and Virendra Pal Singh, "I-2ACK: Preventing Routing Misbehavior in Mobile Ad hoc Networks", International Journal of Computer Applications 62(12):34-39, January 2013.

[25] Wenjia Li, Anupam Joshi, Tim Finin, "SMART: An SVM-based Misbehavior Detection and Trust Management Framework for Mobile Ad hoc Networks", IEEE Transactions on Dependable and Secure Computing (submitted).

[26] Qinghua Li, "Mitigating Routing Misbehavior in Disruption Tolerant Networks", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[27] Ramasamy Murugan and Arumugam Shanmugam, "A Timer Based Acknowledgement Scheme for Node Misbehavior Detection and Isolation in MANET", International Journal of Network Security, Vol.15, No.4, PP.241-247, July 2013.

[28] Tarag Fahad, Robert Askwith, "A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks", The 7th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, pgnet 2006.

[29] "Coping with Node Misbehaviors in Ad Hoc Networks: A Multi-Dimensional Trust Management Approach", The 11th International Conference on Mobile Data Management (MDM 2010), May 2010.

[30] Wei Gong, Zhiyang You, "Trust Based Routing for Misbehavior Detection in Ad Hoc Networks", JOURNAL OF NETWORKS, VOL. 5, NO. 5, MAY 2010.

[31] Amir Khusru Akhtar1, G. Sahoo, "Classification of Selfish and Regular Nodes Based on Reputation Values in MANET Using Adaptive Decision

Boundary", Communications and Network, 185-191, 2013.

[32] S. Soltanali, S. Pirahesh, S. Niksefat, and M. Sabaei, "An Efficient Scheme to Motivate Cooperation in Mobile Ad hoc Networks", In Proc. of ICNS, pages 92–98, 2007.

[33] Enrique Hern_andez-Orallo," CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes", IEEE Transactions On Mobile Computing, Vol. 14, No. 6, 1162-1175, - June 2015.