ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 3, March 2018

Survey on Misbehavior Detection systems in Wireless AdHoc Networks

Gayathri Narayanan[1], Dr. M Rajeswari[2], Mr.Krishna das J[3]
Student, Computer Science, Sahrdaya College of Engineering, Thrissur, Kerala [1]
Associate Professor, Computer Science, Sahrdaya College of Engineering, Thrissur, Kerala [2]
Assistant Professor, Computer Science, Sahrdaya College of Engineering, Thrissur, Kerala [3]

Abstract: Mobile adhoc networks are dynamic in nature and do not have fixed infrastructure to control nodes in the networks. Therefore, it is a big challenge to coordinate among these moving nodes. In addition to this, there may be presence of some selfish nodes which are refused to forward packets to the other nodes which will degrade the performance of the entire network. Identifying those nodes and to eliminate them from the networks is very essential. In this paper, we have discussed Credit based Systems, Reputation based Systems, Acknowledgement based Systems and Audit based Misbehavior Detection Systems in MANET.

Keywords: MANET, Selfish node, Misbehavior Detection system.

I. INTRODUCTION

Mobile Adhoc network (MANET) is formed by wireless mobile nodes that define a temporary network dynamically without using any fixed infrastructure. Flooding and looping are the main problems while transmitting and receiving data in MANET. Because of limited transmission range of wireless networks, multiple network hops are required for one node to swap the data with another across the network. Ad hoc wireless networks find many applications in several areas, due to their quick and economically less demanding deployment. Some of these include: military applications, collaborative and distributed computing, emergency operations and wireless mess networks.

In the absence of supporting infrastructure wireless adhoc networks realize end to end communication in a cooperative manner. In adhoc networks, nodes belong to multiple independent entities, so protocol complaint behaviour cannot be assumed. In order to degrade the network performance, unattended devices can become compromised and drop transit traffic. Also, some selfish nodes in the network misconfigure their devices to refuse forwarding traffic information in order to conserve energy. Some existing methods like credit based, acknowledgement and reputation based schemes for identifying misbehaving node leading to high communication overheads and energy expenditure. These limitations are overcome by AMD which achieves per packet behaviour evaluation without incurring a per-packet per-hop cost. These four methods are reviewed in the next section.

II. REVIEW

Methods proposed for detecting and removing misbehaving nodes from the adhoc network can be,

A. Credit based Systems
B. Reputation based Systems
C. Acknowledgement based Systems
D. Audit based Misbehavior Detection Systems

A. Credit-Based Systems

Credit based methods were also called as incentive based methods. In these methods, selfish nodes were not punished instead unselfish nodes were rewarded for helping other nodes. This stimulates the cooperation of nodes in the network. Credit-based systems were designed to provide incentives for forwarding packets. Buttyan and Hubaux [14] proposed a system in which nodes accumulated credit for every packet they forwarded, and spent their credit to transmit their own packets. To ensure correctness, the credit counter was implemented in tamper-proof hardware. Zhong et al. [18] proposed Sprite, a simple, cheat-proof, credit based system for stimulating cooperation among selfish nodes in mobile adhoc networks, in which nodes were made to collect receipts for the packets that they forward to other nodes. One advantage of Sprite was that it did not require any tamper proof hardware at any node. Whenever the node has had a high-speed link to a Credit Clearance Service

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 3, March 2018

(CCS), it uploaded its receipts and obtained credit. Payments and charges were determined from a game theory perspective. The sender instead of the destination was charged in order to prevent denial-of-service attack in the destination by sending it a large amount of traffic [10][18]. Any node who has ever tried to forwarding a message was compensated, but the credit that the node has received depends on whether or not its forwarding action was successful. Forwarding was considered successful if and only if the next node on the path reported a valid receipt to the CCS. Overhead of the system was found to be small and mobile nodes were cooperative and forwarded the messages effectively.

Crowcroft et al. [15] proposed a scheme used to adjust the credit reward towards traffic and congestion conditions. They have considered how incentives can be integrated into the operation of a mobile ad hoc network and they used pricing mechanisms to recover the cost of resources used at each nodes while forwarding the traffic. These prices are determined in a distributed fashion, and every individual users used algorithms to update their prices based on their bandwidth and power usage. Route with minimum route price is selected for a source to destination connection. That formed a dual algorithm for traffic management within the network. Incentives for collaboration have been provided through the concept of a user having a credit balance, which receives an initial endowment when the user joins the network. The credit balance accumulates notional credit accrued by forwarding traffic for other users, while any traffic generated from a particular user decreases the credit balance based on the cost of forwarding the traffic to its destination. The amount of traffic that a user can generate is directly related to its current credit balance—hence the user's incentive to both act as a transit node for other users and move to locations within the network where it can forward more traffic. While credit-based systems motivated selfish nodes to cooperate, and they provided no incentive to malicious nodes. Such nodes were not intended to collect credit for forwarding their own traffic. Moreover, credit-based systems did not identify misbehaving nodes, thus allowing them to remain in the network indefinitely.

B. Reputation-Based Systems

This section explains methods that are used for punishing the selfish nodes. Selfish nodes are identified and isolated from the network by using this reputation based systems. Most of the approaches in the literature are meant for punishing system rather than rewarding system.

Reputation-based systems use ratings for evaluating the trustworthiness of nodes in forwarding traffic information. These ratings are dynamically adjusted based on the node's observed behavior. In the context of ad hoc networks, Ganeriwal and Srivastava [7] developed a Bayesian model to map binary ratings to reputation metrics, using a beta probability density function. Josang and Ismail [9] proposed a similar ranking system that utilized direct feedback received from one hop neighbors. Michiardi and Molva [12] described the CORE mechanism for computing, distributing, and updating reputation values composed from disparate sources of information. CORE (COllaborative REputation mechanism) was a generic mechanism that would be integrated with any network function like packet forwarding, route discovery, network management and location management [12]. CORE stimulated node cooperation by a collaborative monitoring technique and a reputation mechanism. In this mechanism, reputation was a measure of someone's contribution to network operations. Members that have a good reputation were able to use the resources rather than members with a bad reputation, because they refused to cooperate, which were gradually excluded from the community [12]. Each node was made to compute a reputation value for every neighbor using a sophisticated reputation mechanism that differentiated between subjective reputation (observation), indirect reputation (positive reports by others) and functional reputation (take-specific behavior).

Reputation-based systems use neighboring monitoring techniques to evaluate the behavior of nodes. Marti et al.[10] proposed a scheme which relies on two modules, the watchdog and the pathrater. When a node forwards a packet, the node's *watchdog* verifies that the next node in the path also forwards the packet. The *watchdog* does this by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, then it is considered as misbehaving. The *path rater* uses this knowledge of misbehaving nodes to choose the network path that is most likely to deliver packets. The nodes rely on their own *watchdog* exclusively and do not exchange reputation information with others. Buchegger and Le Boudec [6] proposed a scheme called CONFIDANT, which extended 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 [8] and [16].

Multichannel networks were suffered with highly complex transmission overhearing and motivated by the inadequacy and inefficiency of transmission overhearing, the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 3, March 2018

monitoring approach developed in AMD incurs overhead on a per-flow basis instead of on a per-packet basis, thus having significantly smaller energy expenditure. Moreover, it allows the full customization of the misbehavior criteria for detecting a multitude of selective dropping strategies.

C. Acknowledgment-Based Systems

By keeping the usual meaning of acknowledgments in communication, Acknowledgment-based systems rely on the reception of acknowledgments to verify that a message was forwarded to the next hop. In order to detect misbehaving nodes, Balakrishnan et al.[5] proposed a network-layer scheme called TWOACK, which can be implemented as a simple add-on to any source routing protocol such as DSR, where nodes explicitly send 2-hop acknowledgment messages along the reverse path, verifying that the intermediate node faithfully forwarded packets. TWOACK packets follows a similar functionality as the ACK packets on the Medium Access Control (MAC) layer or the TCP layer. By sending back a two-hop TWOACK packet along the active source route, a node acknowledges the receipt of a data packet. If the sender of a data packet does not receive a TWOACK packet corresponding to a particular data packet that was sent out, forwarding route gets broken due to the assumption of misbehaviour. Based on this claim,accused link will be avoided by the routing protocol from all future routes, resulting in an improved overall throughput performance for the network. 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. [11] improved on TWOACK by proposing 2ACK. Similar to TWOACK, 2ACK technique is based on a simple 2-hop acknowledgment packet that is sent back by the receiver of the next-hop link to verify the cooperation. When Comparing with other approaches to solve the problem, those like the overhearing technique, the 2ACK scheme overcome several problems including ambiguous collisions, receiver collisions, and limited transmission powers. The 2ACK scheme can be used as an add-on technique to routing protocols such as DSR in MANETs. Xue and Nahrstedt [17] proposed the Best-effort Fault-Tolerant Routing scheme, which relies on end to-end acknowledgment messages to monitor packet delivery ratio and select routing paths which avoid misbehaving nodes.

Awerbuch et al. [4] 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. These limitations were overcome by the implementation of Audit based misbehaviour detection systems.

D. Audit-Based Misbehavior Detection Systems

AMD evaluates node behavior on a per packet basis, without any energy expensive overhearing techniques or intensive acknowledgement schemes. Yu Zhang et.al [1] proposed a system called AMD which achieves per packet behavior evaluation without incurring per packet per hop cost.AMD integrates reputation management, trustworthy route discovery and identification of misbehaving nodes. AMD recovers the network operation even if a large fraction of nodes is misbehaving at a significantly lower communication cost and it can detect attacks even though in end to end encrypted traffics.

In audit based misbehaviour detection,one reputation metric is associated with each node and reputation value is calculated for all the nodes.node with low reputation value is eliminated. Nodes with high reputation value is selected and from these nodes using DSR protocol route from sender to receiver is identified. This DSR protocols included an accumulated path reputation field along with RREQ and RREP and TTL.The trustworthiness of route is calculated and a route with highest trustworthiness is selected. Find the selfish node through an audit process. On this audit process the nodes can also lie,so information from honest node is used to identify those who were given a lie. Then this process is mapped to a Supervisory Game theoretical approach.

III. CONCLUSION

This paper discusses various types of misbehavior detection schemes that work in different ways to find out the misbehaving nodes in the network. AMD is better one compared to others since its communication cost is less and it can detect attacks even if the traffic is encrypted and it is also capable for identifying continuous and selective packet droppers.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 3, March 2018

REFERENCES

[1]. Yu Zhang, Loukas Lazos, Member, IEEE, and William Jr. Kozma, "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks",IEEE Transaction on Mobile Computing, 2012

[2]. Vijayakumaran,T. Adiline Macriga, "An Integrated Game Theoretical Approach to Detect Misbehaving Nodes in MANETs", Second International Conference On Computing and Communications Technologies ,pages 173-180,2017

[3]. G. Acs, L. Buttyan, and L. Dora "Misbehaving router detection in link-state routing for wireless mesh networks". In Proc. of WoWMoM, pages 1–6, 2010

[4]. 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

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

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

[7]. 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

[8]. 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

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

[10]. S. Marti, T. Giuli, K. Lai, and M. Baker. "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proceedings. ACM MobiCom, pp. 255–65. , 2000

[11]. 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

[12]. P. Michiardi and R. Molva, "Core: a Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad hoc Networks," Proc. 6th IFIP Conf. Sec. Communication and Multimedia., 2002

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

[14]. L. Buttyán and J.-P. Hubaux,"Enforcing Service Availability in Mobile Ad-Hoc Networks," Proceedings. ACM Mobi-Hoc, pp. 87–96,2000

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

[16]. 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

[17]. 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

[18]. S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," Proceedings. IEEE INFOCOM, pp.1987–97,2003