International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 5, Issue 5, pp 68-73, May-2021

https://doi.org/10.47001/IRJIET/2021.505011

Misbehavior Node detection in Wireless Ad Hoc Networks using Overhearing Techniques

[1]T. N. Sawant, [2]Mitesh Gupta, [3]Vijay Ingle, [4]Divyani Kadam, [5]Sneha Khatke

[1,2,3,4,5]Department of Electronics and Telecommunication, Bharati Vidyapeeth College of Engineering, Navi Mumbai, India

***Abstract* - The nodes in the wireless network co-operate with each other in data transmission. The data packets transfer from source to destination nodes. Some nodes in the network participate well in routing operations such as the route discovery, and route maintenance. But the node behaves selfishly in forwarding the data packets due to wastage of a battery power, and other resources. The wireless network has open challenge to identify and separate the misbehave nodes in the networks. The misbehave nodes lead to a high energy consumption and an overhead in the network. To overcome the limitations of the wireless Ad Hoc networks, in this research paper, we have proposed two novel approaches. In the first approach, the source node calculates the packet forward ratio and identifies misbehave nodes in the network. This approach is called the Overhearing Based Misbehavior Detection (OMD) approach. Where In first approach we have to calculate the packet forwarding ratio in which neighbor overhears transmissions and its own transmissions, then our second approach is Autonomous Agent-based Misbehavior Detection approach where the AAMD scheme generates the secret key to verify the misbehavior of the node using the agent. It also utilizes the past behavior of the node to identify possibilities. We have proposed both the approaches to achieve the better QoS and to reduce the network overhead and delay. The implementation is based on NS2 software and comparison of the simulation results of the proposed approaches.**

Keywords: MANET, OMD, AAMD, PFR.

I. INTRODUCTION

The Mobile Ad Hoc Networks (MANET) are self-organizing networks without any pre- infrastructure. The nodes in MANET communicate with each other. The network has multiple routes to solve the communication range problems. In MANET source node can send the packets to the destination node using the intermediate nodes [1]-[3]. The intermediate nodes can receive the packets and forward packets to neighbor nodes. The deployed in a different environment and does not have any control mechanisms.so the nodes move freely from one location to another location. Due to this nature, the nodes are easily manipulated by attackers. The MANET has open challenges such as the effect of misbehaving nodes. The misbehave nodes have different characters such as denial of forwarding packets, false routing information, packet dropping [4]-[6]. The misbehaving node leads to degrade the performance of the network. In wireless networks misbehave node also have different types like an overload misbehave node is of lack of resources Software fault node is called fault misbehave node and it can easily launch denial of service attacks.

Many approaches are presented to detect the misbehaving nodes in wireless networks. But these approaches mostly depend on the hardware of the system without hardware support, credit-based approaches are not recognized as misbehave nodes [8]-[11]. The Reputation-based approaches are on transmission overhearing which is expensive and leads to communication overhead [12]-[14]. The Acknowledgement based approaches had more communication overhead by the issuance of packet acknowledgment [18]-[20][21]. High communication overhead due to audit process and delay in process of route discovery in Audit Based Approach [23]. Quality of Service Support (QoS): This is a set of service requirements that must met with the network which carries the packet flow from the source to its destination It is governed by the service requirements of end-user applications and is expected to guarantee users a set of measurable pre-specified service features in terms of end-to-end performance, such as delay, bandwidth, throughput, packet loss, delay change.

Packet Delivery Ratio: This is the total number Packets transmitted by source over total number of packets received by destination. The basic idea of PDR is to choose a reliable route. 100% delivery that means all packets sent by the receiver are received by source node. Packet end-to-end delay: the average time a packet takes the network in traverse. A network is a measure of the successful transmission rate in the end-to-end throughout network, and is usually defined as the number of data packets successfully delivered to its final destination per unit time. The mobile Ad Hoc network is designed to be scalable. As the network grows, different protocols work differently. Routing traffic increases as the network grows. an important measure of the scalability of the protocol is called routing overhead. A network is defined as

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 5, Issue 5, pp 68-73, May-2021

https://doi.org/10.47001/IRJIET/2021.505011

the number of total routing packets transmitted over the network, expressed in bits per second, or packets per second.

The rest of the paper is structured as follows. Section II provides a review of the related work on the approach to detecting misbehave nodes to improve QoS in wireless applications. Section III. Provides problem definition and implementation of the proposed procedure. Section IV Provides the implementation simulation result Section V concludes the paper with guidelines for future work.

II. RELATED WORK

Various techniques have been developed to detect the dropping misbehavior in wireless Ad Hoc network [8][9][25][26]. The proposed schemes can be classified as:

1.1 Credit Based Systems

In credit-based frameworks, a few credits are given to transitional nodes, at whatever point a hub advances bundles or give administrations to different nodes in the organization. The credits got can be utilized by the hubs to communicate their own traffic. L. Buttyan et al. [11] have proposed two models which can be utilized in credit-based plans.

Firstly, Packet Trade Model in which each middle hub gives a few credits to past hub and purchase parcels from it and sells the bundles to next node for additional credits. The objective hub bears generally speaking expense of sending the bundles. Furthermore, Packet Purse Model in which credits are stacked into a bundle before it is sent by the sender hub.

Every one of the middle hubs which forward the parcel gets a few credits for doing it. On the off chance that every one of the credits gets depleted prior to arriving at the objective hub, at that point the bundle is dropped. L.Buttyan et al. [11] have proposed a plan inwhich every hub in the organization keeps a counter of credits of nuggets known as nugget counter. Another credit based plot named Sprite, was proposed by Zhang et al. [10].

In Sprite, hubs gather receipts forgot and sent bundles. Hubs give these receipts to Credit Clearance Service (CSS) and receive credits consequently.

1.2 Reputation Based Systems

The reputation of a node is determined by its neighbor by noticing the parcel sending conduct of the node. Reputation figured is utilized in the framework for assessing the reliability of nodes in sending traffic and recognizing the bad conduct of dubious nodes [12]-[16]. This data is at that point proliferated all through the organization so the recognized getting into a mischief node can be taken out from the network. Marti et al.[26] have proposed a plan that contains two significant modules, named watch dog and to identify furthermore, relieve steering rowdiness in MANET, individually. Utilizing the revelation of the guard dog module, path rather rates every way in the reserve and chooses the way which evades node misconduct.

1.3 Acknowledgment Based Systems

Acknowledgment put together frameworks with respect to the gathering of affirmation in order to check that, a message is sent straightaway jump. Balakrishnan et al. [19] have proposed a TWO ACK plan in which a node sends a 2-jump affirmation message, at whatever point they get a bundle, along with the converse way which checks that the middle node has sent the bundle.

Samreen et al.[27] have proposed a methodology which employees two methods: 2ACK strategy and Principle of Flow of Conservation (PFC) method which is utilized in corresponding to the empower of the discovery of nodes that display parcel dropping conduct. The outcome produced by the first strategy is utilized by the second procedure to create the rundown of acting mischievously nodes.

1.4 Review Based Systems

Review based Misbehavior Detection method [23] incorporates three modules: (a) Reputation module is mindful for the board of notoriety estimation of nodes in the organization also, for refreshing the standing dependent on the information given by the review module. (b) Route revelation module is mindful for discovering the most dependable way among accessible ways on the premise of way notoriety worth and way determination factor. (c) Audit module distinguishes the getting into mischief nodes in the way utilizing reviewing measures.

This interaction is sped up dependent on the standing qualities which are given by the standing module. AMD assesses node misconduct on per parcel premise without utilizing catching procedure or affirmation conspire. AMD can likewise, identify dropping assault of particular nature.

In this work, initially, a neighbor catching based misconduct location conspire is proposed. Besides, a self-sufficient specialist based misconduct location conspire is proposed. Inspiration behind the work is to improve correspondence overhead furthermore, recognizable proof postponement in a remote specially appointed organization.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 5, Issue 5, pp 68-73, May-2021

https://doi.org/10.47001/IRJIET/2021.505011

III. PROPOSED METHODOLOGY

3.1 Problem Statement

The wireless networks are interconnected with many no. of nodes. Ad Hoc wireless networks deployed in emergency environments. The emergences are different types such as environmental disasters industrial accidents and battle fields. The facility of Ad Hoc networks is to work on limited resources and it does not require any pre-infrastructure for operations. Due to this Ad Hoc networks usage increase in real time applications. But the Ad Hoc networks have open issues due to its nature. The node in the network can change the behavior easily and compromised with the attacker nodes. Many approaches are introduced to identification misbehave nodes in the networks. However, these approaches are achieved better results but unable maximize the QoS in the networks. The main problem of system is that unable to reduce overhead and delay in the network.

3.2 Proposed Methodology

In proposed methodology, we employed two main approaches for identification of misbehavior node in the network. Overhearing Based Misbehavior Detection (OMD) approach has been implemented. Then Autonomous Agent Based Misbehavior Detection approach implemented. In Figure 1 presented architecture of proposed approach.

A. Overhearing based Misbehavior Detection

The OMD approach depends on Packet Forward Ratio between the source and destination. It maintains all neighbors nodes PFR in the network. The PFR is used to identify the misbehavior node in the network. In proposed network, source node broadcast RREQ packets in the network. All nodes in the networks receive the RREQ packet and then forward to neighbor node in the network. Once the destination node receives the RREQ packet it will respond with RREP packets with shortest routing path. The source node maintain the status of complete route path from source to destinations. Source node sends the data packets to the destination node using the route determined. Source node continuously monitors the performance of path PS−>D based on the packet delivery ratio η. If it detects that this ratio is less than some predefined threshold value η0. It will send a control packet ReqPFR at time t to request all the intermediate nodes to calculate Packet Forwarding Ratio (PFR) of their own and their neighbors based on the number of packets forwarded Packet to source and number of packets received pr for a time duration. t1. When this control packet reaches to the destination node, it generates a control packet RepPFR after time duration t1. Destination node calculates PFR of itself and its neighbors and appends this value to the control packet ReqPFR and sends the packet in reverse direction to the source node. All intermediate nodes append their calculated PFR value to the packet and send it to their previous node. Source node updates its matrix based on the values in the control packet RepPFR. Source node checks the matrix and finds the node for which calculated values of Packet Forwarding Ratio conflict with each other and declares that node as misbehaving node [8].

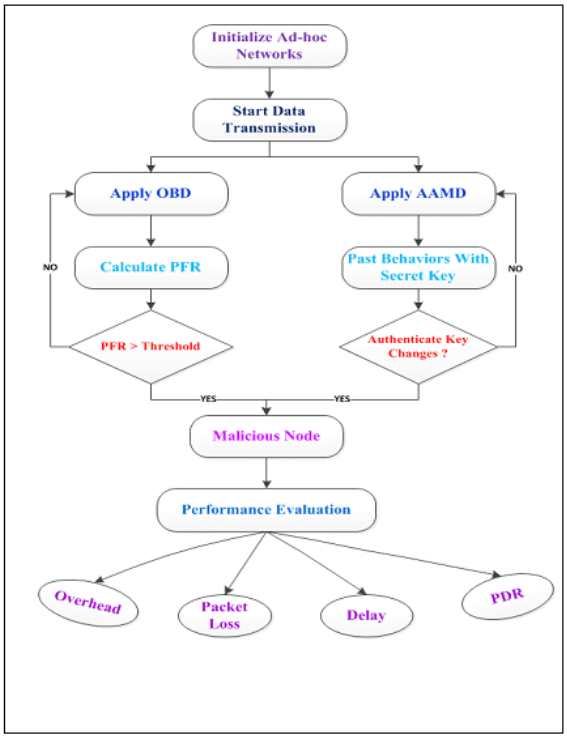

Figure 1: Proposed Architecture

B. Autonomous Agent Based Misbehavior Detection (AAMD)

The AAMD approach has been presented in which an agent resides at each node, which will be activated to calculate PFR of that node [27].It is using RSA algorithm which generates the key to activate the agent residing at the node. This activation key will be requested by the source node in presence of misbehavior. Source node first request to generate the secret keys before data transmission of data packets. It maintains the information of every node id and secret key. If both values match, then generated secret key and computed PFR value of the node is provided to source node. Source node compares the calculated value with minimum acceptable value of PFR. If the calculated value is less than the minimum acceptable value, the node is identified as misbehaving node and the selection probability matrix is updated accordingly.

IV. RESULT ANALYSIS

NS2 version 2.35 is used to implement the proposed AAMD approach for enhancing data transmission and misbehave node detection in wireless networks. With proposed AAMD approach, the performance of the wireless

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 5, Issue 5, pp 68-73, May-2021

https://doi.org/10.47001/IRJIET/2021.505011

network with misbehave node detection is studied through simulations. The observations presented in this section. as a well behaving node and matrix is updated accordingly.

As shown in Figure 2, the simulation time is taken from 0 seconds to30 seconds. As simulation time is increased, the delay performance statistics are recorded for the proposed system. The results are compared with standard system. As the simulation time increase the proposed AAMD approach shows significantly less delay. In the rest of the simulation time, the proposed system showed comparable performance over the CBS and OMD.

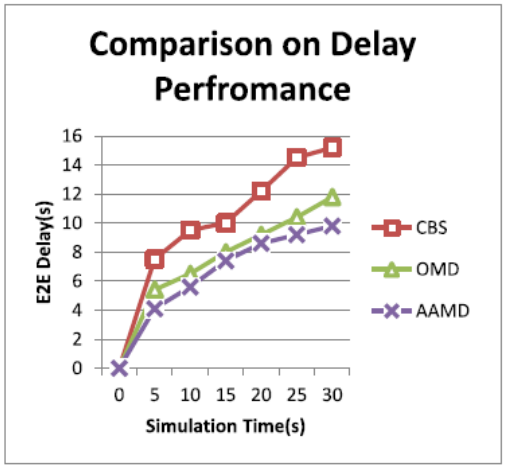

Figure 2: Delay Performance

Packet delivery ratio recorded for CBS, AMD and AAMD approaches is presented in Figure 3. The simulation time considered is from 0 seconds to 30 seconds is increased gradually in 5 seconds interval. The PDR value is increased for three approaches as simulation time is increased. This is an important observation. The second trend involved is that, the PDR of the proposed system is higher than the standard one in all time intervals. Thus, the proposed approach outperforms the existing one with respect to PDR.

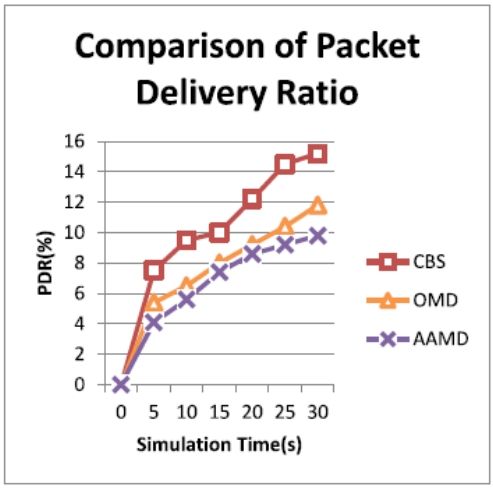

Figure 3: PDR Performance

As shown in Figure 4, the simulation results in terms of throughput are presented. The simulation time is considered from 0 seconds to 30 seconds with 5 seconds interval. The overhead of the proposed system is recorded as 28 consistently. While the same for the standard systems CBS and OMD recorded as 70, 42 respectively. There is significant difference between the two approaches. The proposed approach have less overhead compared to existing approaches CBS and OMD.

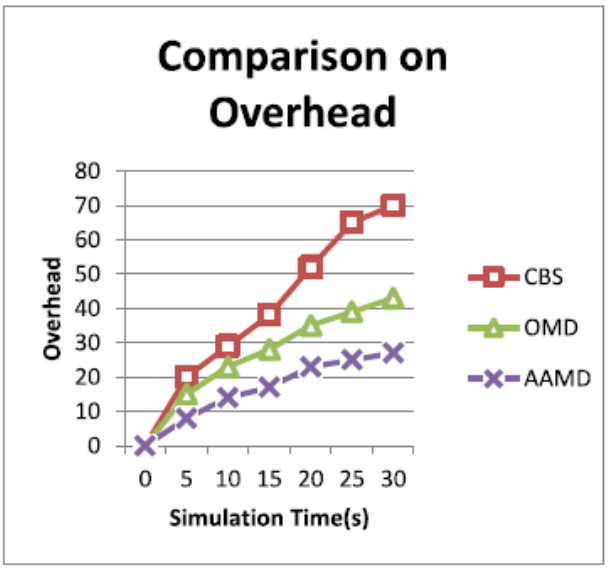

Figure 4: Overhead Performance

V. CONCLUSION

We have proposed two techniques for misbehavior detection in wireless Ad Hoc networks. Firstly, an Overhearing based Misbehavior Detection (OMD) technique is proposed which is based on behavior evaluation by neighboring nodes. The OMD technique reduces the identification delay by transmitting few control packets for identifying the misbehaving nodes in the network. Secondly, an Autonomous Agent based Misbehavior Detection (AAMD) technique is proposed. The AAMD technique achieves up-to 25% less communication overhead than the AMD technique. Also, the identification delay has been reduced (using AAMD) significantly for identifying misbehaving nodes using autonomous agents in the network. Further, investigation may be done to develop an isolation scheme to isolate the detected misbehaving nodes from the network.

REFERENCES

[1] Visconti and H. Tahayori, “Detecting misbehaving nodes in manet with an artificial immune system based on type-2 fuzzy sets, International Conference for Internet Technology and, Secured Transactions, , ICITST’09, pp. 1–2,2009.

ISSN (online): 2581-3048
Volume 5, Issue 5, pp 68-73, May-2021
https://doi.org/10.47001/IRJIET/2021.505011

[2] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing Ad Hoc wireless networks," in Proc. of ISCC, 2002.

[3] R. R. Rout and S. K. Ghosh, "Enhancement of lifetime using duty cycle and network coding in wireless sensor networks ," IEEE Transaction on Wireless Communication, vol. 12, no. 2, pp. 656–667,2013.

[4] Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile Ad Hoc networks," IEEE Communications, , vol. 14, no. 5, pp. 85– 91, 2007.

[5] A.B. Abderrahmane Baadache, "Fighting against packet dropping misbehavior in multi-hop wireless Ad Hoc networks," J. Network and Computer Applications, vol. 35, no. 3, pp. 1130–1139, 2012.

[6] D. Djenouri and N. Badache, "On eliminating packet droppers in manet: A modular solution," Ad Hoc Networks, vol. 7, no. 6, pp. 1243–1258, 2009.

[7] F. Kargl, a. Klenk, M. Weber, and S. Schlott, "Advanced detection of selfish or malicious nodes in Ad Hoc networks," in 1st European Workshop on Security in Ad Hoc and Sensor NetworksHeidlberg, Germany, Aug 5-6, 2004, 2004.

[8] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgement based approach for detection of routing misbehavior in manets," IEEE Transactions on Mobile Computing, vol. 6, no. 5, pp. 536–550, 2007

[9] S. Zhang, J. Chen, and Y.R.Yang, "Sprite : A simple cheat-proof, credit based system for mobile Ad Hoc networks," in Proc. of INFOCOM, 2003, pp. 1987–1997.

[10] L. Buttyan and J. P. hubaux, "Stimulating cooperation in self organizing mobile Ad Hoc networks," Mobile Net. and Application, vol. 8, no. 5, pp. 579–592, 2003.

[11] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentive for collaboration in mobile Ad Hoc network," in Proc. of WiOpt, 2003.

[12] S. Ganeriwal, L. Balzano, and M. Srivastava, "Reputation based framework for high integrity sensor networks," ACM Transactions on Sensor Networks, vol. 4, no. 3, pp. 1–37, 2008.

[13] Q. He, D. Wu, and K. Khosla, "Sori: A secure and objective reputation based incentive scheme for Ad Hoc networks," in In Proc. of WCNC, 2004.

[14] S. Buchegger and J. Y. L. Boudec, "Self policing mobile Ad Hoc networks by reputation systems," in IEEE Comm. Magazine, 2005, pp. 101–107.

[15] L. Miranda, H.and Rodrigues, "Preventing selfishness in open mobile Ad Hoc networks," in Proc. of Seventh CaberNet Radicals Workshop, 2002.

[16] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol: Cooperation of nodes, fairness in dynamic Ad Hoc networks," in Proc. of MobiHoc, 2002.

[17] P. Michiardi and R. C. Molva, "A collaborative reputation mechanism to enforce node cooperation in mobile Ad Hoc networks," in The 6th IFIP Communication and Multimedia Security Conference, Portoroz, Slovenia, Sep 26-27, 2002, 2002.

[18] K. Balakrishnan, J. Deng, and P. K. Varshney, "Twoack: Preventing selfish node in mobile Ad Hoc networks," in Proc. of WCNC, 2005.

[19] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotary, and H. Rubens, "Odsbr: An on-demand secure byzantine resilient routing protocol for wireless Ad Hoc networks," ACM Transactions on Information Syatem Security, vol. 10, no. 4, pp. 11–35, 2008.

[20] Y. Xue and K. Nahrstedt, "Providing fault- tolerant Ad Hoc routing services in adversial enviornment," Wireless Personal Communications, special issue on security for next generation communications, vol. 29, no. 3, pp. 367–388, 2004.

[21] A.S. Anandukey and C. M., "Detection of packet dropping attack using improved acknowledgement based scheme in manet," International Journal of Computer Science Issues I, vol. 7, no. 1, pp. 12–17, 2010..

[22] S. Manvia, L. B. Bhajantrib, and V. K. Vagga, "Routing misbehavior detection in manets using 2ack," Journal of Telecommunication and Information Technology, vol. 4, no. 1, pp. 105–111, 2010.

[23] Y. Zhang, L. Lazos, and W. J. Kozma, "Amd : Audit baesd misbehavior detection in wireless Ad Hoc networks," IEEE Transactions on Mobile Computing, 2013.

[24] R. Perrig, A. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," in CryptoBytes, vol. 5, no. 2, 2002, pp. 2– 13.

[25] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile Ad Hoc networks," in In Proc. MobiHoc, 2000

[26] S. Samreen and G. Narasimha, "An efficient approach for detection of node misbehavior in a manet based on link behavior," IEEE International Journal of Advance Computing Conference, pp. 588–592, 2012.

ISSN (online): 2581-3048

Volume 5, Issue 5, pp 68-73, May-2021

https://doi.org/10.47001/IRJIET/2021.505011

[27] L. Buttyan and J. P. Hubaux, "Enforcing service availability in mobile Ad Hoc wans," in In Proc. MobiHoc, 2000.

[28] V. Bharghavan, A. Dermers, S. Shenker, and L. Zhang, "Macaw: A medium access protocol for wireless lans," in In Proc. of ACM SIGCOMM '94, 1994.

[29] D. Johnson, A. Maltz, and J. Broch, "The dynamic protocol for mobile Ad Hoc networks," in Mobile Ad Hoc Network Working Group, IETF, 1999.

[30] G. Simon, P. Vlgyesi, M. Marti, and A. Ldeczi, "Simulation-based optimization of communication protocols for large-scale wireless sensor networks," IEEECA, 2003.

Citation of this Article:

T. N. Sawant, Mitesh Gupta, Vijay Ingle, Divyani Kadam, Sneha Khatke, "Misbehavior Node detection in Wireless Ad Hoc Networks using Overhearing Techniques" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 5, Issue 5, pp 68-73, May 2021. Article DOI https://doi.org/10.47001/IRJIET/2021.505011

****

