International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Impact of Finding Selfish Nodes in Manet

V Anandkumar, Kalaiarasan T R, Ratheesh Kumar A M

Abstract*: *The nodes that operate in the self-organized functions of Mobile Ad hoc Networks (MANETs) participate in the network but increase the energy and resources consumption. As some nodes are non-cooperative with others in the network, it is necessary that those nodes have to be removed. Active researches are conducted to deal with those selfish nodes that are non-cooperative. Methods/ Statistics: Our paper analyzes by comparing the 2ACK method simulated using hash chain one-way scheme with digital signature and DSR methods. Findings: The simulation analysis suggest that a considerable percentage of packets delivered of 2ACK method is greater when compared with Digital signature or any other DSR methods but has the capability in finding a considerable number of selfish nodes present in the network. Applications/ Improvements: the 2ACK scheme can be used to control the network overhead using the authentication schemes and can be enhanced to monitor the video traffic can be monitored.

***Keywords* : *MANET, misbehaving Nodes, Digital Signature, MAC layer, one way hash chain*.**

I. INTRODUCTION

A group of host nodes transmitting either directly or using intermediate nodes as routers via wireless channel does not depend on pre-existing infrastructure as the network nodes randomly change the topology instantly and unpredictably can be termed as MANET. The activities of nodes include discovering random topology and packet delivery to an individual or a network. The architecture of MANET differs from a low power consumes fixed network and a high mobility varying network. MANETs are classified as closed MANET, where all mobile nodes cooperate among them to achieve a common goal or as open ones, where each individual node has its own goal but share their resources to achieve global connectivity. However, energy is consumed by few resources when nodes in the network continue to cooperate in the self organized functions. The misbehaving nodes utilize the resource of other intermediate nodes but deny their resources. Wireless transmission still remains the major source of consuming energy in MANET. As the selfish node has to conserve its energy, it may not cooperate with other nodes by sharing or forwarding data packets. Few methods are proposed to discover and alleviate the selfish nodes from the network. By monitoring the wireless medium , the [1] watchdog technique can be used to find the nodes that are not sharing its resources while path rater technique makes the well behaved nodes to avoid misbehaving nodes in selecting a best route to deliver the packets. The watchdog mechanism is a silent observer that verifies whether the intermediate nodes send the data packet to the next node. The selfish nodes have to be detected and removed by all the other nodes by using the 2ACK scheme to detect the after effects of the node's misbehavior. When the receiver receives a data packet from source node via intermediate node, to indicate the successful delivery, a success message is received by the sender from the receiver thus reducing the overhead created due to the routing behavior. The nodes are checked for its behavior for a certain time period and the selfish nodes are detected. The paper gives an indication of simulating the working of 2ACK scheme with the traditional methods by using some parameters to evaluate the performance of the proposed work.

Manuscript published on 30 August 2019.
*Correspondence Author(s)
Dr Anandkumar V, Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India.
Kalaiarasan T R, Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India.
Ratheeshkumar A M, Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India

II. ARCHITECTURE OF 2ACK

The issue of less overhead in watchdog mechanism will get an outcome of ambiguous and receiver collisions and reduced power transmission. So it is obvious that we have to detect and remove the [4] selfish nodes which act as a router for delivering the packets ti the intermediate node or link.

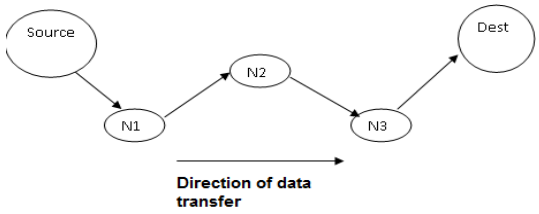

Figure 1 Operation of 2ACK scheme

2.1 Components of 2ACK Scheme

2ACK technique is used to discover and mitigate the [2] selfish nodes by incorporating an acknowledgement packet for successfully delivering the data packet to the initiator via supplementary link. The operation of 2ACK scheme in Figure 1 provides three nodes N1, N2 and N3 for delivering the data packets successfully. An optimal route is found from source node S to destination node D via the route discovery phase implemented in [7] DSR protocol. A data packet transmitted to N3 from N2 via N2 using route discovery mechanism remains ambiguous as whether N3 has successfully received the data packets. This confusion remains even when selfish nodes does not exist. The scheme requires a normal acknowledgement from the receiving node N3when it sends the data packets to the initiator node N1.

N2 Intermediate node	N3 Receiving node	Tpkts packets Transmitted	Mpkts packets Missed	LIST List of data packets

Figure 2 Components of the Monitoring node

When a 2ACK packet w.r.to. N3 arrive before the timer set, the intermediate node is removed from the network else Tpkts would be incremented. On receipt of data packet, N3 decides whether to send a return packet 2ACK back to to N1. This mitigates the selfish nodes by avoiding and reducing the overhead caused due to routing mechanism.

The missed 2ACK packets Mpkts is compared with threshold value Rmis by the source node after observing the link from N2 to N3 for a certain period. If Mpkts > Rmis, the link from N2 to N3 is denoted as selfish and N1 sends out an RERR packet reporting that the link is a misbehaving link. Rmis should be greater than Mpkts to avoid the misbehaving nodes when using a technique that uses partial acknowledgment. The link is separated as and when the node receives or overhears the RERR and marks it as denied nodes and does not allow further in the network. When any node transmits the data packet, it first checks the list of denied nodes and avoids those routes that have misbehaving links. [6][8]

III. AUTHENTICATION OF 2ACK SCHEME

If the acknowledgement packet 2ACK was received from N3 to N1 via node N2 in Figure 1, without security, a selfish node N2 can perform fabrication of 2ACK packets and inform that they were transmitted by N3. So, [7] we need a digital signature algorithm to alleviate 2ACK packets sent repeatedly.

As the method exhibits fairness, it is impossible to forge without knowing the security key of node N3 and integrity of the information can be easily found. The digital signature algorithm is implemented using techniques namely RSA but are costly for mobile nodes which are [3] constrained by resources. A novel algorithm is used for implementing against traditional security attack such as Denial of Service (DoS). The hash computing function in [9] hash chain algorithm takes an input of dynamic length and produces an static output of bit string.

$H:\{0,1\}^{*}\rightarrow\{0,1\}^{\rho}$, where ρ is the length in bits.

The following characteristics are needed for a hash function H to be ideal:

- A variable length for input
- Fixed output length
- It should be collision free.
- The hash function can be computed for a given value x.

The free from collision characteristics confirms that the hash function results are unique. Examples include MD5 [14] and SHA1 [15].

A node randomly generates an initial value x $\varepsilon\{0,1\}^{\rho}$ and calculates the hash value. The initial value in the chain h_0 is given as x. So it becomes necessary to check all the elements using the existing authenticated mechanism. One way of avoiding the problem of false alarms is hash chain mechanism where a trusted authority is engaged to authenticate the packet sent form node N3 to N1. But the main issue in MANET is that there is no any central server to play the role of trusted certificate authority. There are two alternatives to send the h_n element to N1 from N1 namely transmission extension and multi path transmission respectively. Using the first technique, transmission power is increased by N3 to send the h_n element to N1 without the knowledge of N2 but it consumes large amount of energy from N3. In the second technique, node N3 floods a packet carrying h_n element through variable paths to the intermediate nodes. MAC value calculated by N3 on the basis of $h_{i-1,}[N_{2,}N_{1,}ID]h_{i-1}$ combined with hi value is sent along with the 2ACK packet sent.

The analysis shows that a low computational cost of 2ACK scheme when compared over other schemes. So it becomes necessary that length of each element in the node and the size has to be considered as the major factors of communication overhead. When chosen nominally, we can get less transmission overhead.

IV. CALCULATION OF TIMEOUT FOR RECEIVING 2ACK PACKETS

Assume that τ is the timer used for successful operation of 2ACK packet reception. When timer expires, the missing packet Cmis would be incremented before 2ACK packet was received. If the value of τ is too small, then wrong acknowledgements would be received else large memory is needed by the monitoring node. To avoid temporary link failures, it becomes necessary to set the value of τ to be large. So it becomes essential that the time-out operation should satisfy the condition $\tau > 4*[\text{1-hop\_T}_{\text{Delay}}]$, where 1-hop_$T_{Delay}$ includes the delayed transmission of packet, random back-off delay at MAC layer, delay in processing the data and the retransmission delay.

V. SIMULATION ANALYSIS

We present the simulation analysis of 2ACK over the DSR protocol and Digital signature algorithm for evaluating some performance measures.

5.1 Simulation and Performance Metrics

The comparison study is simulated and implemented using Network Simulator (NS-2). The observation period T_{obs} has been set an initial value of 0:10 seconds. The 2 ACK scheme used an initial value of T_{ack} as 0:10 sec, T_{mis} as 0:10 sec and the value of τ as 0:20 sec. The channel has a initial data rate of 10 Mbps and has a packet size of 512B. Transmission range of the node N=200m. The simulation area is randomly distributed in a 600m by 600m flat area with a initial value of N as 50 nodes. The comparative analysis of 2ACK scheme over the traditional schemes uses the following metrics:

i.) Packet Delivery Ratio, PDR = Nd/ Ns, where
Nd - Number of packets received by the recipient
Ns - Number of packets sent by the initiator.

ii) The overhead caused by the routing protocol Ro= Arp/ Atd, where

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Arp= No of routing related packets (RERR, 2ACK, RREQ or RREP)
Atd= No of forwarded/ transmitted packets

iii) The number of Selfish nodes not sharing the resources and non-cooperating.

The simulation analysis deals with the fact that TCP senders have the ability to detect the failure while delivering the data packets in end- to-end node automatically. This may lead to stopping or slowing down of the initial node which happens when intermediate nodes becomes selfish nodes and deals with the missing acknowledged packets from destination. Hence, it becomes necessary that the successful delivery of total packets to be a more useful metric for performance comparison. The simulation analysis of the three metrics is provided in Figures 3-5. The analysis suggests that the percentage of packets delivered of the proposed 2ACK scheme performs to a considerable extent when compared with traditional schemes. The proposed scheme has a greater routing overhead and the average delay in receiving the acknowledgement packets is nominal in the proposed scheme when comparing the other two schemes.

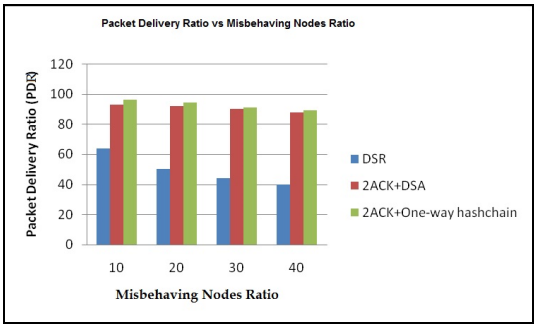

Figure 3. Packet Delivery Ratio vs Misbehaving Nodes Ratio

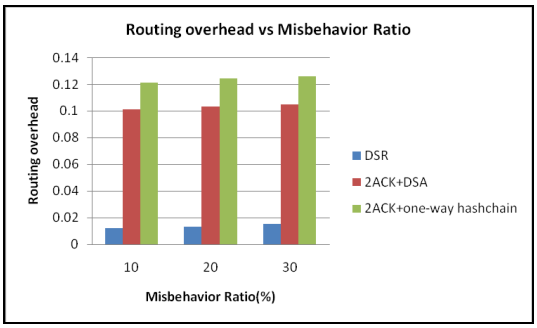

Figure 4. Routing Overhead vs. Misbehavior Ratio

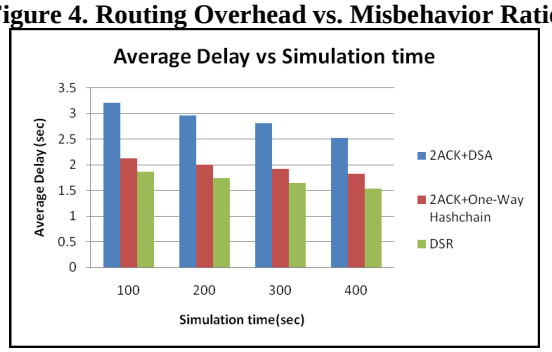

Figure 5. Average Delay vs Simulation Time

VI. CONCLUSIONS AND FUTURE WORK

Manet has been found wanting in the area of communication related to military forces. The end-to-end node depends on intermediate nodes to perform networking functions as cooperation is the key for the successful delivery of data packets. So it becomes necessary that the routing activities of intermediate nodes have to be monitored for finding the misbehaviour of selfish nodes and mitigating them. In this regard, 2ACK scheme alleviates the selfish nodes thereby providing a secure route for delivery of packets and overcoming the possible ambiguous and receiver collisions and available power that is used for transmission.

To reduce the issue of receiving wrong acknowledgement methods, we have used digital signature scheme and the performance is compared with 2ACK scheme. The simulation analysis shows that the percentage of packets delivered by the proposed 2ACK mechanism seems better when compared with the traditional digital signature method. By using the various authentication schemes, 2ACK method has the capability to control the network overhead. In future, the video traffic can be monitored by using 2ACK scheme.

REFERENCES

1. V.Anandkumar and S.Subramanian, 'Security Based on Context -Aware Adaptive Routing in Delay Tolerant Mobile Ad Hoc Networks', Australian Journal of Basic and Applied Sciences, vol. 9, no. 7, pp. 669 –676,2015
2. V. Anandkumar, S. Subramanian and P.Thangam, "Improving the Performance Using Shared Spread Protocol in Issue Guarantee Protocol over Delay Tolerant Networks', International Journal of Applied Engineering Research, ISSN 0973-4562, vol.10, no.23, pp. 43737-43740,2015.
3. L.M. Feeney and Nilsson, "Investigating the Energy Consumption of a Wireless Network Interface in an AdHoc Networking Environment," Proc. IEEE INFOCOM, 2001.
4. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom, Aug.2000.
5. S. Buchegger and J.-Y. Le Boudec Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proc. MobiHoc, June 2002.
6. D. Johnson, D. Maltz, Y.C. Hu, and J. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR),"Internet draft, Feb. 2002.
7. S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proc. MobiHoc, June 2002.
8. R.L. Rivest, "RFC 1321—The MD5 Message-Digest Algorithm," technical report, MIT Laboratory for Computer Science and RSA Data Security,Inc.,Apr.1992.
9. D. Eastlake and P. Jones, "RFC 3174—US Secure Hash Algorithm 1(SHA1)," technical report, Motorola and Cisco Systems, Sept.2001.
10. Kalaiarasan T R, Anandkumar V, Ratheesh Kumar A M," Sales Forecasting using RNN", International Journal of Innovative Technology and ExploringEngineering(IJITEE) ISSN: 2278-3075, Volume-8 Issue-9, July 2019.

AUTHORS PROFILE

Dr V Anandkumar received his Bachelor degree in Engineering CSE at Tamilnadu College of Engineering, Karumathampatti, Master degree in Engineering, CSE at Arulmigu Kalasalingam College of Engineering, Krishnan Koil, Doctorate in ICE at Anna University, Chennai in 1998, 2001 and 2017 respectively. He is currently a Professor at Sri Krishna College of Engineering and Technology. His specific areas of interests are ADHOC networks, Artificial Intelligence and Cloud Computing. He has published more than 10 papers in reputed international journals and two books.

Kalaiarasan T R received his Bachelor degree in Information Technology at Ganadipathy Tulsis Engineering College, Vellore and Master degree in Mainframe Technology at Anna University, Coimbatore in 2010 and 2012 respectively. He is currently an Assistant Professor at Sri Krishna College of Engineering and Technology. His specific areas of interests are Data Analytics and IoT. He has published 5 papers in reputed international journals.

Ratheesh Kumar A M received his Bachelor degree in Engineering CSE at Paavai Engineering College, Namakkal and Master degree in Engineering IT at SNS College of Technology, Coimbatore in 2008 and 2011 respectively. He is currently an Assistant Professor at Sri Krishna College of Engineering and Technology. His specific areas of interests are Data Analytics and IoT. He has published 5 papers in reputed international journals.

Retrieval Number: J98670881019/19©BEIESP
DOI: 10.35940/ijitee.J9867.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)