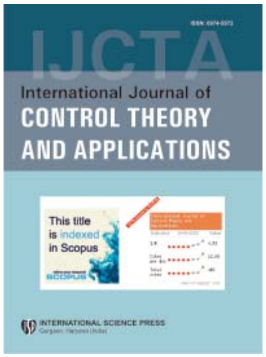

International Journal of Control Theory and Applications

ISSN : 0974–5572

© International Science Press

Volume 10 • Number 27 • 2017

A Secure Acknowledgement-Based Adaptable System for MANETs

A. Anitha[a] R. Suji Pramila[a] and P. Swetha[b]

[a]Noorul Islam Centre for Higher Education, Department of Computer Science and Engineering, Kumaracoil, Tamilnadu, India

E-mail: anidathi@yahoo.co.in, sujisymon @gmail.com

[b]Jeppiaar Engineering College, Department of Computer Science and Engineering, , Chennai, Tamilnadu, India

E-mail: swetha.p.ananth@gmail.com

Abstract: Mobile Ad hoc networks are the dynamic temporary network without any infrastructure and centralized administration. The main challenging issues of the wireless Ad hoc networks are security and QoS. This work aims on the secure and high efficient adhoc network protocol using rate adaptation scheme. Rate adaptation is a rate control mechanism which selects the optimum transmission rate at a given time. To improve the throughput a node must adjust its transmission rate for the dynamically changing environments. Ideally, the transmission rate should be adjusted according to the channel condition. This is a destination based approach where the destination node checks the channel status and gives an acknowledgement to the source node. Upon receiving the acknowledgement the source node decides whether to increase/decrease the rate. If the channel status is good enough to increase the rate then the source node increases the rate and perform End to End transmission. If bad, again the channel status is checked by the destination till it is good to increase the rate for End to End transmission. For securing the acknowledgement and to find where the acknowledgement has lost Hop-Hop transmission is done. Hop-Hop transmission is done for the first occurred nodes which send both the channel status and the acknowledgement. If the acknowledgement is lost then the hop-hop transmission is done for the nodes other than the first occurred nodes and performs end to end transmission. This work reduces the communication overhead, increases the security and increases the performance of the network.

Keywords: *Rate Adaptation; Adhoc Networks; Security; styling; insert (key words)*

1. INTRODUCTION

Ad hoc is the Latin word, means “for this (only)”. The Wireless Ad hoc networks are a group of wireless nodes, communicates through a wireless medium without a base station or AP. The Ad hoc networks are the distributed, decentralized networks. Each node in the network has the responsibility of routing, security and to solve the network problems. There is no centralized control, each node with the wireless transceiver, acts as the client and the server for routing as well as the protected transmission of the data packet to the destination node. The nodes in the Ad hoc networks communicate with each other in a common area using a specialized feature known as routing. The nodes in ad hoc network have a limited transmission range so they every node requests the help of the neighborhood node for forwarding the packets to the destination. Thus the node in ad hoc network does the task of the router as well as the hosts.

Initially the ad hoc networks are used in the military or the disaster relief applications. But today these networks are used commercially for the internet applications of the nodes which are not in the range of wireless AP. The nodes in the ad hoc network are mobile and generally will have a dynamic topology. The dynamic topology network will insightfully have great network characteristics. Due to the wireless medium and the infrastructureless nature, the network creates a lot of problems which are different from the fixed networks. The main problems in the ad hoc network are routing, power efficiency and security.

For the significant assignment applications, for example the military applications the network security is critically important. In addition with the security the adaptation of the rate according to the dynamic nature of the MANET to reach the designated destination with high performance improvement is too important. This paper proposes a secure acknowledgement-based adaptable system for transmitting the highly important information in the critical mission applications with a novel routing method. The adaptability is done by the rate adaptation method. Rate adaptation is a critical and an unspecified mechanism which exploits Multirate capability at the physical layer Wong et al. (2006). The fundamental challenge of the rate adaptation is the estimation of the channel condition regardless of the presence of various mobility caused by fading, hidden nodes and mobility. To cope up with the dynamically changing environment and the channel conditions the rates should be adapted effectively for the improvement of the system performance. This paper used the closed loop rate adaptation scheme, acknowledgement based method for supporting the secure acknowledgement based transmission in the MANETs.

This paper is organized as follows: Section I presents a general introduction, Section II with the previous research, Section III proposes the new acknowledgement based secure algorithm for MANETs, Section IV with the results and discussion and Section V concludes the paper.

2. PREVIOUS RESEARCH

Watchdog scheme was proposed by [1] to improve the performance of the MANET in the presence of malicious nodes. This method mainly serves as an Intrusion Detection system for identifying the malicious node misbehaviors in the MANET. This system listens the next hop transmission for finding the misbehaviors of the malicious node and increases its failure count if there is misbehavior in a particular node for the secure transmission within a particular period of time. This method cannot find the misbehavior of the nodes in collisions, collusions, false misbehavior report, limited transmission power and partial dropping.

To overcome the issues in the watchdog scheme TWOACK [] scheme was proposed by Liu et al. This scheme in which the nodes receiving each packet has to send back the acknowledgement packet to the node that is two hops away from it. This scheme overcome the issues such as collision, limited transmission power problems of the watchdog scheme but increases the network overhead and usage of more power for the redundant transmission of the acknowledgement packet leads to the degradation of the entire network. AACK was proposed by Sheltami et al [] based on the TWOACK scheme. This method integrates the TACK (similar to TWOACK scheme) and End-to-End acknowledgement. The network overhead was reduced by the AACK scheme when compared to the TWOACK scheme.

3. PROPOSED WORK

The proposed secure based adaptable scheme combines the rate adaptation scheme with the acknowledgement based scheme in the MANET for improving the performance than the existing secure systems. The rate adaptation scheme used is the closed loop rate adaptation scheme which adapts the rate based on the feedback from the destination. This is the feedback based method which suits the closed loop rate adaptation scheme, combines the channel status feedback for the efficient improvement of the performance of MANET.

This system is based on the feedback and the acknowledgement from the destination node. If the data and Acknowledgement transmitted is received successfully, then the End-to-End acknowledgement is done between the source and the destination node. If any failure of either data or the acknowledgement, then the hop by hop acknowledgement is done for the first occurred nodes to find the node where the data or the acknowledgement has been dropped.

If the acknowledgement process done is the End to End acknowledgement, the destination node checks the status of the channel condition by checking the SNR value with the threshold. If the SNR value is less than the threshold value then the channel condition is estimated as good and gives a feedback to the source node to increase the rate to improve the performance in the current channel condition. If the SNR value is greater than the threshold value, then the feedback is given as to decrease the rate for the current channel condition. The end to end acknowledgement process exchanges the feedback for increasing/decreasing the rate for the estimated current channel condition based on the estimator SNR.

The End to End acknowledgement process is shown in Fig.2. S and D represents the source node and the destination node. The I, *j*, *k*, and *l* represents the intermediate nodes. Pd_1 and Pa_1 represents the data frame and the acknowledgements respectively. Fig. 3 shows the end-to end feedback process. Here the pd_1 and F_1 represents the data frame and the corresponding feedback respectively.

If the acknowledgement process is the Hop by Hop process, then the source node has to check both the received acknowledgement as well as the feedback from the destination node as well as the intermediate nodes. If both the acknowledgement and the feedback is received by the source then it performs an End to End acknowledgement process between the source and destination. If any one of the acknowledgement or the feedback or both was missed then it performs a hop by hop acknowledgement process other than the first occurred nodes. The Fig. 4 and Fig. 5 show the hop by hop feedback process to the source node as well as by the intermediate nodes respectively. Both the end to end and hop by hop acknowledgement process performs the rate control process for increasing or decreasing the rate based on the current channel condition for improving the throughput performance.

Algorithm

Step 1: Source node transmits the data frame to the destination.

Step 2: Destination receives the data frame.

Step 3: Destination checks that the ACK is received.

3.1. If yes, End to End ACK is done between the source and the destination.

3.2. Else Hop by Hop ACK is done for the first occurred nodes.

Step 4: After End to End ACK the Destination checks the channel status

4.1. If (SNR < Threshold) then the rate is increased by the source

4.2. Else (SNR > Threshold), decrease the rate and then End to End ACK is done.

Step 5: If Hop by Hop ACK then the source checks whether it receives the feedback and ACK

5.1. If received then End to End ACK is done between the source and the destination.

5.2. Else Hop by Hop ACK is done by the nodes other than the first occured.

Step 6: Both End to End ACK and Hop by Hop ACK checks the channel status after receiving ACK and FEEDback

6.1. If the channel status is good (SNR < Threshold), then the rate is increased

6.2. Else the rate is decreased.

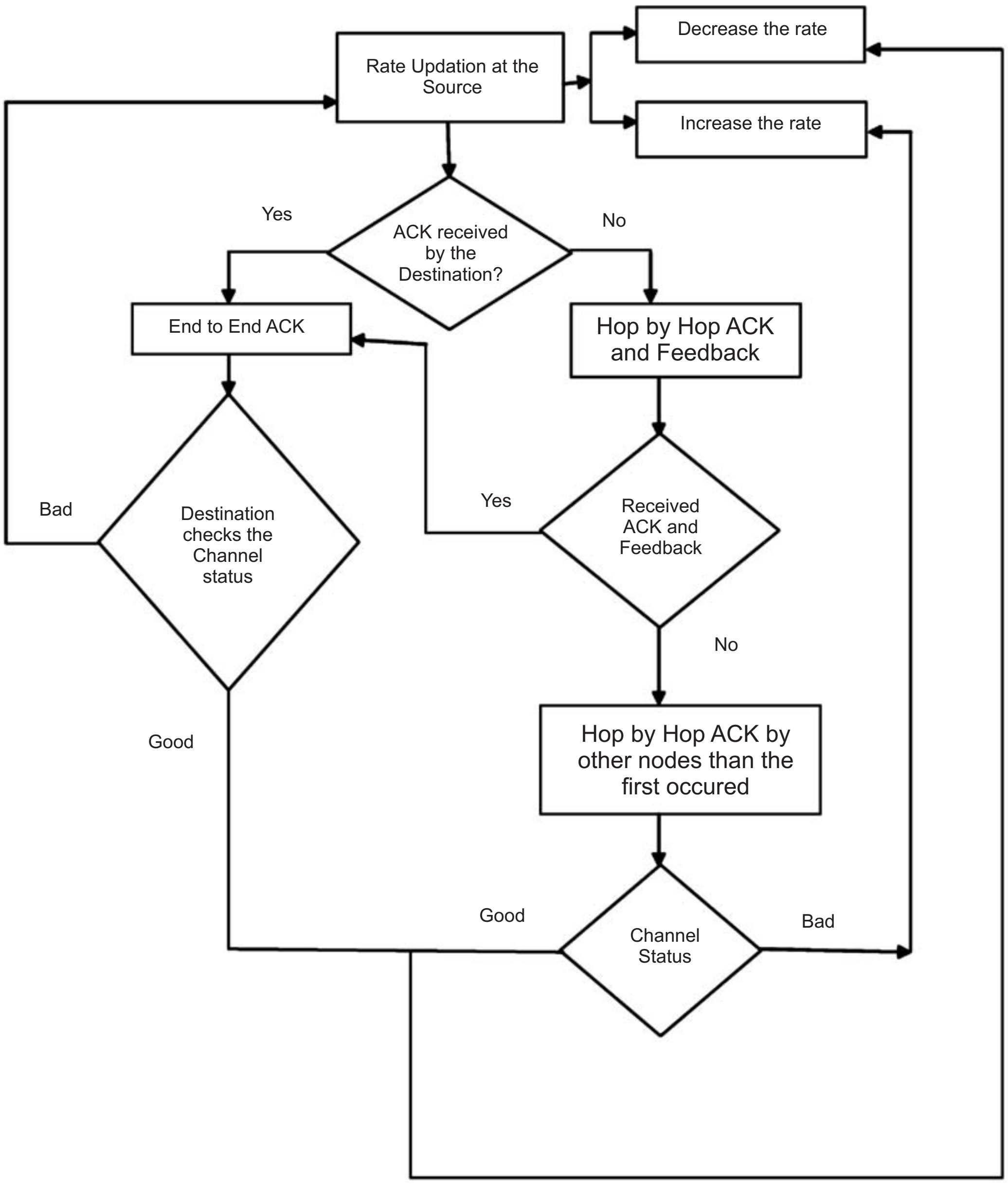
Rate Updation at the Source
Decrease the rate
Increase the rate
ACK received by the Destination?
Yes
No
End to End ACK
Hop by Hop ACK and Feedback
Destination checks the Channel status
Bad
Good
Received ACK and Feedback
Yes
No
Hop by Hop ACK by other nodes than the first occured
Channel Status
Good
Bad

Figure 1: Flow Diagram for the proposed work

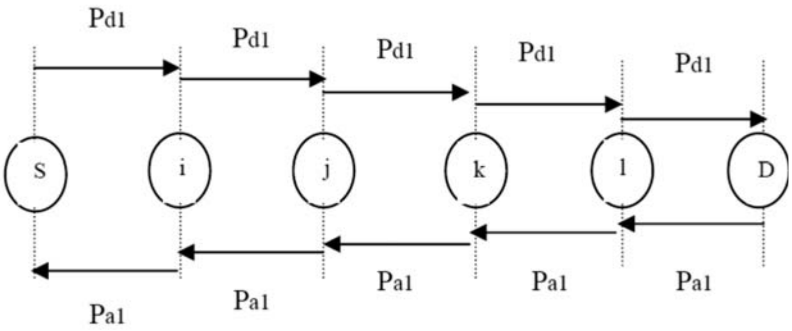

Figure 2: End-End Acknowledgement

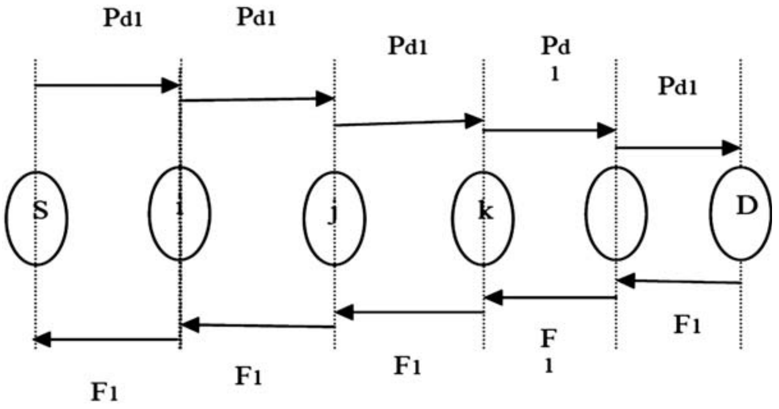

Figure 3: End-to-End Feedback

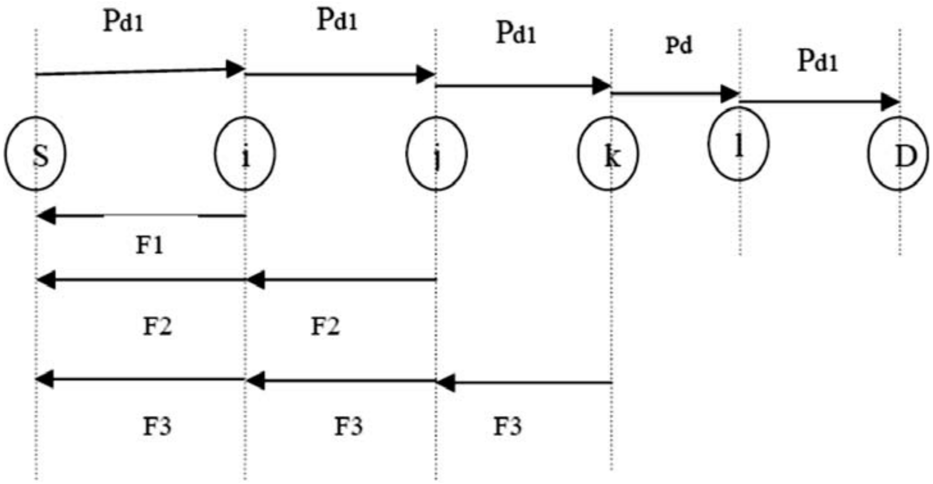

Figure 4: Hop by Hop Feedback (source node)

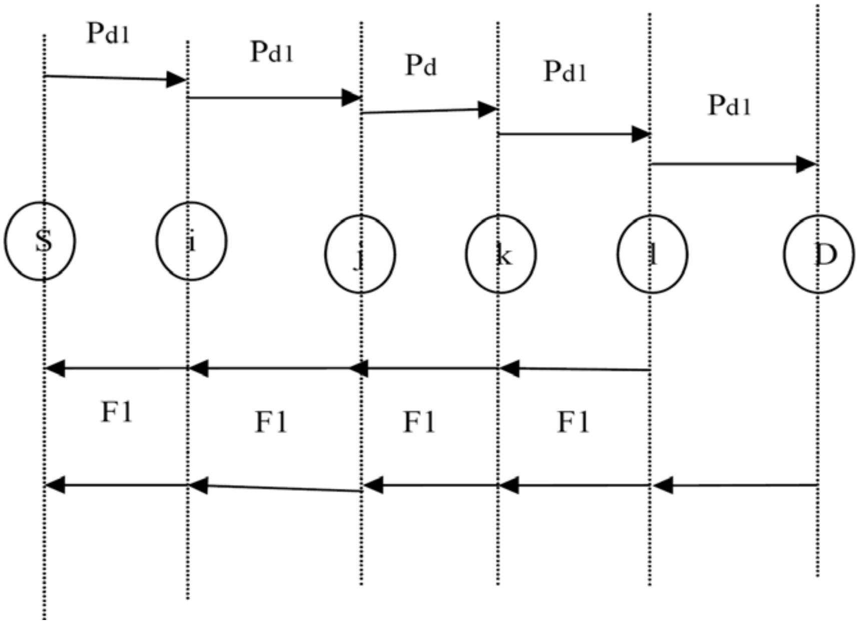

Figure 5: Hop by Hop Feedback (intermediate nodes)

4. PERFORMANCE EVALUATION

The performance of the proposed method is analyzed using the NS 2.34 network simulator under the Ubuntu environment. The maximum nodes configured are 50 with the work space of size 670X670 m. This configuration setting allowed a maximum of four hops between the nodes. The physical and the 802.11 MAC layers are allowed in the wireless NS2 extension. The speed of the mobile nodes used are 20 m/s. User Datagram protocol with a constant bit rate is used with the packet size of 512 bytes. The performance parameters used are the throughput and the packet delivery ratio. Throughput is the number of packets transmitted per unit time and the packet delivery ratio is the ratio of number of packets received successfully by the destination node to the number of packets transmitted by the source node.

This work is analysed with the presence of various malicious nodes and is compared with the existing TWOACK system. The performance of the proposed system outperforms well than the existing because of the acknowledgement based on the hop by hop and the end to end with the rate control method and is depicted in Fig. 6 .

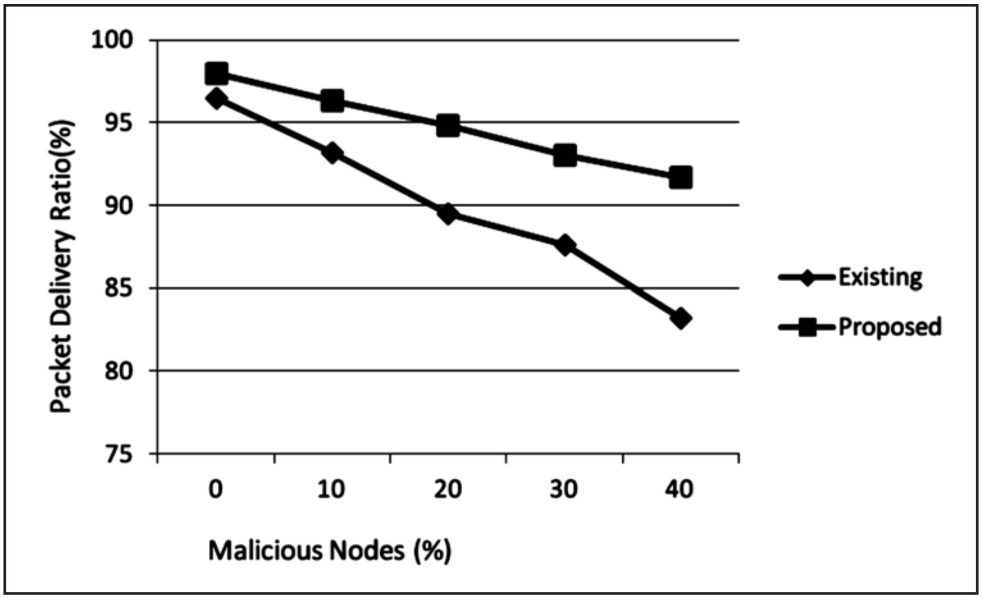

Figure 6: Packet Delivery Ratio

5. CONCLUSION

This is the hybrid method which integrates the security and the rate control method for the secure and adaptable transmission in MANETs. Here the hop by hop and end to end acknowledgement based systems are used for the security and the closed loop rate adaptation scheme is used for the adaptability. The performance of the proposed work is analyzed on packet delivery ratio in the presence of malicious nodes that gave a better performance than the existing TWOACK method.

REFERENCES

[1] J .S. Lee- “A Petri net design of command filters for semiautonomous mobile sensor networks”.[Apr-2008]

[2] K.Liu,J.Deng,P.K.Varshney, And K.Balakrishnan -“An acknowledgement- based approach for the detection of routing misbehavior in

[3] S . Marti , T . J. Giuli , K . Lai ,and M . Baker, -“Mitigating routing misbehavior in mobile ad hoc networks”.[Mar-2000]

[4] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," *IEEE Trans. Ind. Electron.*,vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[5] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127.New York: Springer-Verlag, 2012, pp. 659–666.

[6] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535–541.

[7] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security*. New York: Springer-Verlag, 2008.

[8] L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[9] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modelingand optimization of a solar energy harvester system for self-powered wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 7,pp. 2759–2766, Jul. 2008.

[10] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[11] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.