ISSN: 2393-8528

IJICSE
Open Access

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 4 Issue 3; May-June-2017; Page No. 24-29

ROUTING MISBEHAVIOR DETECTION IN MANET USING 2ACK

A. Nithya

M.Sc.,M.Phil., Assistant Professor, BCA Department,

KG College of Arts and Science,

nithya.a@kgcas.com

Received 20 March 2017; Accepted 28 April. 2017

ABSTRACT

This paper proposes routing detection in Manet's mistreatment 2ACK theme. Routing protocols for MANETs area unit designed supported the idea that each one participating nodes area unit totally cooperative. However, due to the open structure and scarcely out there battery-based energy, node could exist. Within the existing system, there is a possibility that once a sender chooses associate degree intermediate Link to send some message to a destination, the intermediate link may cause issues like, the intermediate node might not forward the packets to destination, it's going to take terribly long time to send packets or it's going to modify the contents of the packet. In MANETs, as there's no retransmission of packets once it is sent, care should be taken to not loose packets. We have analyzed and evaluated a way, termed 2ACK theme to discover and mitigate the impact of such routing misbehavior in MANETs setting. It's supported an easy 2-hop acknowledgment packet that's sent back by the receiver of the next-hop link. 2ACK transmission takes place for under a fraction of information packets, however not for all. Such a selective acknowledgment is meant to cut back the extra routing overhead caused by the 2ACK scheme

General Terms: Security, Wireless, 2ACK

Keywords: Cmiss,Rmiss,Pm

Introduction

A mobile Ad hoc network (MANET) could be a assortment of mo-bile nodes (hosts) that communicate with one another via wireless links either directly or wishing on alternative nodes as routers. The operation of MANETs doesn't rely up on preexisting infrastructure or base stations. Network nodes in Manet's area unit absolve to move. Therefore, the network topology of a MANETs could amendment chop-chop and unpredictably. All network activities like discovering the topology and delivering knowledge packets need to be executed by the nodes themselves either severally or collectively. Counting on its application, the structure of a Manet could vary from a little, static network that's highly power-constrained to a large-scale, mobile, highly dynamic network. There are unit 2 varieties of MANETs: closed and open [1].

In a closed Manet, all mobile nodes join forces with each other towards a standard goal, like emergency
search/rescue or military and enforcement operations. In AN open Manet, totally different mobile nodes with different goals share their resources so as to make sure international connectivity. However, some resources area unit consumed quickly as the nodes participate within the network functions. For in-stance, battery power is taken into account to be most significant in a mobile surroundings. A personal mobile node could attempt to take pleasure in alternative nodes, however refuse to share its own resources. Such nodes area unit known as self-serving nodes or misbehaving nodes and their behavior is termed as misbehavior. One among the most important sources of energy consumption within the mobile nodes of MANETs is wireless transmission. A self-serving node could refuse to forward knowledge packets for alternative nodes so as to conserve its own energy [2], [3].In MANETs, routing misbehavior will severely degrade the performance at the routing layer.
Specifically, nodes may participate within the route discovery and maintenance processes however refuse to forward knowledge packets. However will we sight such misbehavior? a way to build such detection method more economical

Corresponding author: A. Nithya |

(i.e., with less management overhead) and accurate (i.e., with low warning rate and incomprehensible detection rate). I have a tendency to analyze the 2ACK technique [4] to sight such misbehaving nodes or links. Routes containing such nodes will be eliminated from thought. The supply node will be ready to opt for AN acceptable route to send its knowledge. The 2ACK theme could be a network-layer technique to sight misbehaving links and to mitigate their effects. The 2ACKscheme detects misbehavior through the employment of a brand new kind of acknowledgment packet, termed 2ACK. A 2ACK packet is allotted a hard and fast route of 2 hops (three nodes) within the opposite direction of the info traffic route. During this work, we provide safety features to 2ACK, wherever confidentiality of the message is checked by confirmatory the initial hash code with the hash code generated at the destination. The rest of the paper is organized as follows. Section 2discusses connected add this space. Section three describes the proposed work. Section four presents the simulation procedure, performance parameters and therefore the results of the proposed work.

1. RELATED WORK

The security downside and also the misconduct downside of wire-less networks together with MANET's are studied by many researchers. Varied techniques are planned to prevent stinginess in MANETs. a number of the connected works area unit as follows. The work given in [5] explains detection of malicious nodes by the destination node, isolation of malicious nodes by discarding the trail and bar information packets by victimization dispersion techniques. The work given in [4] describes the performance degradation caused by egoistic (misbehaving) nodes in MANETs. They have planned and evaluated a way, termed2ACK, to find and mitigate the result of such routing misbehavior. The work given in [6] presents cooperative, distributed intrusion detection design for MANETs that's meant to address some challenges. The design is organized as a dynamic hierarchy, during which information acquisition happens at the leaves, with intrusion detection information being incrementally collective, reduced, analyzed, and related because it flows upward towards the foundation. The work given in [7] explains the matter of identification of misbehaving nodes and refusing to forward packets to a destination. they need planned a reactive identification mechanism that doesn't have confidence continuous overhearing or intensive acknowledgment techniques, however is simply activated in the event of performance degradation. The work given in [8] proposes a general resolution to packet dropping misconduct in mobile circumstantial networks. The solution permits watching, detecting, and analytic the droppers. The work given in [9] proposes signal strength based mostly routing for wireless circumstantial networks. It uses signal strengths on the multi hop to spot stable route from supply to destination in an advertisement hoc networks. A stable route helps to reduce management packets overhead throughout route maintenance and avoids route interruptions1**.**

PROPOSED WORK

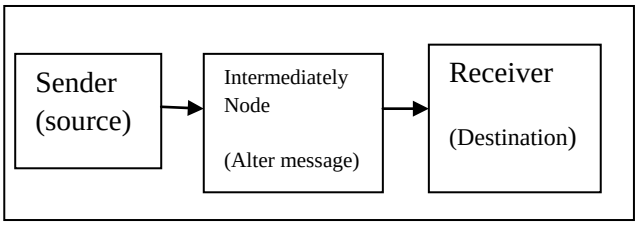
The planned system is employed to notice the wrongdoing routing exploitation 2ACK and additionally check the confidentiality of the info message in Manet's atmosphere. Here, we tend to used a theme known as 2ACK theme, wherever the destination node of consecutive hop link can challenge a two hop acknowledgement known as 2ACK to point that the info packet has been received with success. The planned work (2ACK with confidentiality) is as follows.

- If the 2ACK time is a smaller amount than the wait time and therefore the original message contents aren't altered at the intermediate node then, a message is given to sender that the link is functioning properly.
- If the 2ACK time is additional than the wait time and therefore the original message contents aren't altered at the intermediate node, then a message is given to sender that the link is misbehaving.
- If the 2ACK time is over the wait time and therefore the original message contents area unit altered at the interme- diate node, then message is given to sender that the link is misbehaving and confidentiality is lost.
- If the 2ACK time is a smaller amount than the wait time and therefore the original message contents area unit altered at the intermediate node then, a message is given to sender that the link is functioning properly and confidentiality is lost. At destination, a hash code are generated and compared with the sender's hash code to examine the confidentiality of message. Hence, if the link is misbehaving, sender to trans- university messages won't use it in future and loss of packets is avoided. This section presents system model, and functioning theme.

3.1. *System Model*

In the existing system, there is a chance that once a sender chooses associate intermediate link to send some message to destination, the intermediate link might provide issues like the intermediate node might not forward the packets to destination, it should take terribly durable to send packets or it should modify the contents of the packet. In MANETs, as there's no retransmission of packets once it's sent, thence care is to be taken that packets aren't lost. Noting that a misbehaving node will either be the sender or the receiver of the next-hop link, I've targeted on the matter of sleuthing misbehaving links rather than misbehaving nodes victimization 2ACK theme. Within the next-hop link, a misbehaving sender or a misbehaving receiver includes a sim ilar adverse eject on the information packet. it'll not be forwarded more. The result's that this link is labeled. Our approach is employed to debate the significantly simplifiion of the routing detection mechanism and conjointly checking the confidentiality of the message in MANETs environment.

Figure1 shows the system model of the projected work. The assorted modules within the system model are as follows.



Module 1:

Sender module (Source node). The task of this module is to browse the message so divide the message into packets of forty eight bytes long, send the packet to receiver through the intermediate node and receive acknowledgement from the receiver node through the intermediate node. Once causing each packet the "Cpkts" counter is incremented by one. 2ACK time is compared with the wait time. If 2ACK is a smaller amount than wait time, "Cmiss" counter is incremented by one. The magnitude relation of "Cmiss" to "Cpkts" is com- pared with the "Rmiss" (a threshold ratio). If it's but "Rmiss", link is functioning properly otherwise misbehaving.

Module 2:

Intermediate module (Intermediate node). The task of this module is to receive packet from sender, alter/don't alter the message and send it to destination. Get2ACK packet from the receiver and send 2ACK packet to sender.

Module 3:

Receiver module (Destination node). The task of this module is to receive message from the intermediate node, do away with destination name and hash code and decrypt it. Compare the hash code of supply node and destination node for security purpose. Send 2ACK to supply through the intermediate node.

A. At node N1 while (true) **do**

- Read the destination address;
- Read the message;
- Find the length of the message.

Cmiss=0, Cpkts=0, WT=20 ms, d=0.2,
2ACK Time=Current Time (Acknowledgement ac- cepted time) – Start Time.
while (length > 48 bytes) **do**
Take out 48 message packet;
Length = length – 48;
Encode message using hash function;
Send message along with the hash key;
Cpkts++ ;
Receive 2ACK packet;
if (2ACK time > WT) **then**
Cmis+;
end

B. At node N2 while (true) **do**
Read message from source N1
if (Alter) **then**
Add dummy bytes of characters;
Process it and forward to destination N3;
Receive 2ACK from N3 and send it to N1;
else if (Do not Alter) **then**
Process it and forward to destination N3;
Receive 2ACK from N3 and send it to N1;
end

C. At node N3 while (true) **do**
Read message from N2;
Take out destination name and hash code;
Decode the message;
Send 2ACK packet to N2;
end

D. At N1 and N3 parallel while (true) **do**
if ((Cmiss/Cpkts)>d and (hash code of source msg) ! = (hash code of destination msg)) **then**
Link is misbehaving and the confidentiality is lost;
end
if ((Cmiss/Cpkts)<d and (hash code of source msg) ! = (hash code of destination msg)) **then**
Link is working properly and the confidentiality is lost;
end
if ((Cmiss/Cpkts)>d and (hash code of source msg) = (hash code of destination msg)) **then**
Link is misbehaving;
end

if ((Cmiss/Cpkts)<d and (hash code of source msg) = (hash code of destination msg)) **then**
Link is working properly;
End

4. SIMULATION

4.1. Simulation Model

Our simulation model consists of N range of nodes. The nodes square measure elect at random in MANETs setting. The first node is usually assumed because the supply node and therefore the last node is assumed because the destination node.

Remaining nodes square measure assumed because the intermediate nodes (e.g., N = seventy nodes, therein first, i.e., N1 is assumed as supply node and last, i.e., N70 is assumed because the destination node and N2 to N69 square measure assumed as the intermediate nodes). we have a tendency to have used a number of the functions in our simulation model.

• Pm – the fraction of nodes that square measure misbehaving. The misbehaving nodes square measure elite among all network nodes randomly;
• Rmiss – the edge to see the allowable magnitude relation of the whole variety of 2ACK packets lost to the whole variety of knowledge packets sent;

• R2ack – the acknowledgement magnitude relation, the fraction of knowledge packets that square measure acknowledged with 2ACK packets (maintained at the 2ACK sender).

4..2.SimulationProcedure

To illustrate a number of the results of simulation, we've thought-about the subsequent setting variables as follows: N = ten to ninety for different cases, Pm = 0, 0.1, 0.2, 0.3, 0.4, WT = twenty ms and R2ack = zero.05, 0.2, 0.5, and 1.

Begin
1) Arbitrarily generate variety of nodes N.
2) Calculate the acknowledgement time within the absence of misbehaving nodes.
3) Calculate for the chosen parameter for different values of Pm starting from zero to zero.4 and find the quantity of misbehaving nodes.
4) Expect some delay and also the calculate constant parameter for different R2ack values starting from zero.05 to 1.

5) Apply the projected theme.
6) Calculate the performance parameters.
7)Generatethegraphs.
End

4.3.PerformanceParameters

I have used the subsequent parameters to live the per- formance of the 2ACK theme in MANET's.

• Packet delivery magnitude relation (PDR) – the magnitude relation of the num- ber of packets received at the destination and also the variety of packets sent by thesupply.
• Routing overhead (RO) – the magnitude relation of the number of routing connected transmissions (such as misbehaviour report, 2ACK etc) to the number of information transmissions. The number is in bytes. each forwarded and transmitted packets square measure counted.
• 2ACK time – it measures the time needed to receive the 2ACK packet from destination node to supply node throughout the absence of misbehaving nodes.
• 2ACK time1 – it measures the time needed to receive the 2ACK packet from destination node to supply node throughout the presence of some misbehaving nodes.
• turn out – it measures the general performance of the 2ACK theme with regard to the wrongful conduct magnitude relation.

4.4. Results and Discussion

Figure 2 shows the packet delivery ratio versus misbehavior ratio. The packet delivery ratio (PDR) of the 2ACK scheme with different acknowledgment ratios (R2ack). The varied Pm

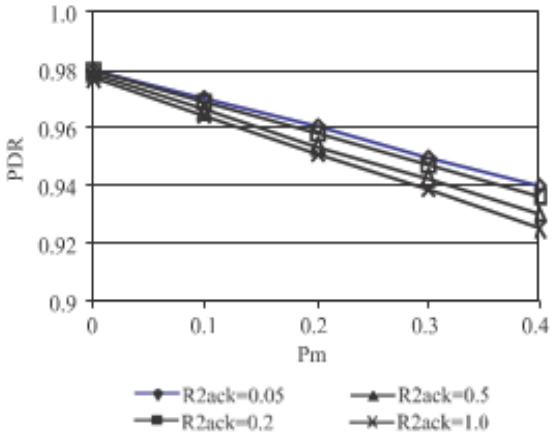


Fig. 2: Packet delivery ratio (PDR) versus misbehavior ratio

(Pm) that most packets were delivered when Pm = 0 (no misbehaving nodes). The packet delivery ratio decreases as Pm increases. The 2ACK scheme delivered over 90% of the data packets even when
Pm = 0.4.
The acknowledgment ratio R2ack was set to 0.05, 0.2, 0.5 and 1 respectively. R2ack does not appreciably affect the PDR performance of the 2ACK scheme.

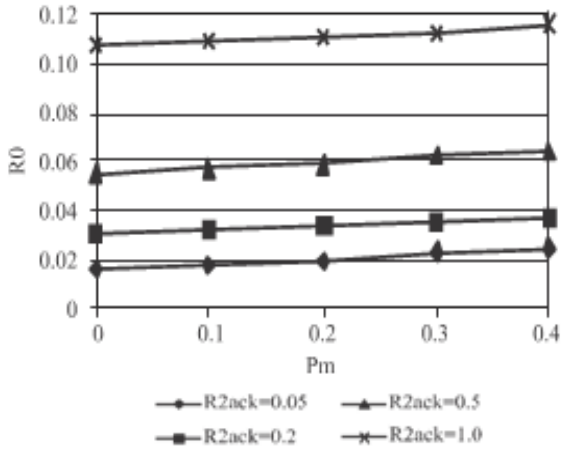


Fig. 3: shows the routing overhead (RO) of the 2ACK scheme with different acknowledgment ratios, R2ack. We varied Pm from 0 (all of the nodes are well behaved) to 0.4 (40% of the nodes are misbehave). Here, I compare routing overhead of the 2ACK scheme with different R2ack values. Overhead of the 2ACK scheme is highest when R2ack = 1. This is due to the large number of the 2ACK packets transmitted in the network.

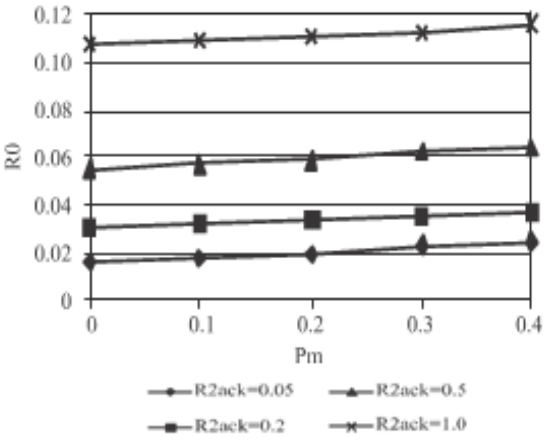


Fig. 4: shows Routing Overhead(RO)

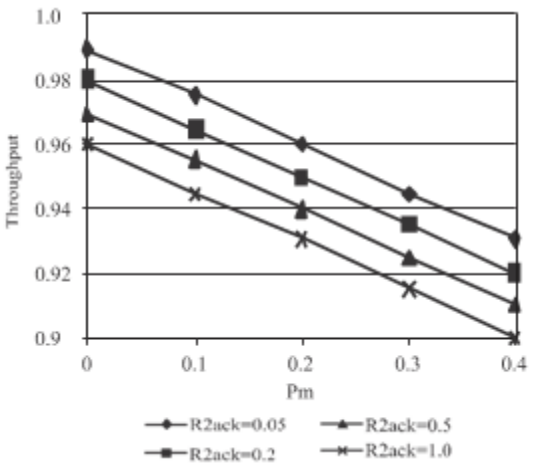


Fig. 4: show the relative throughput of the 2ACK scheme with dfferent knowledge ratio's. Here I have compared the throughput of the 2ACK scheme and also the different behaviours of the ratio values

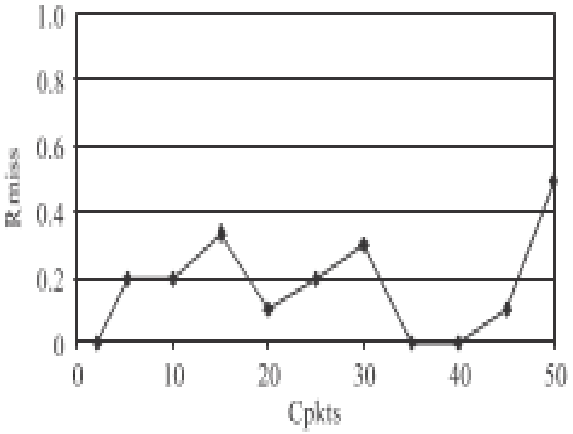


Fig. 5: shows that graph of 2ACK miss ratio (Rmiss).Cmiss depends upon 2ACK Time.

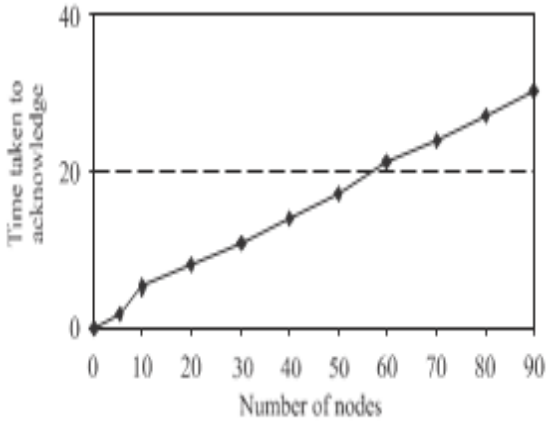


Fig. 6: shows Number of nodes vs time taken to acknowledge

5. CONCLUSION

Mobile ad hoc networks have been an area for active re-search over the past few years, due to their potentially widespread application in military and civilian communications. Such a network is very keen about the co- operation of all its members to perform networking functions. This makes it extremely liable to selfish nodes.Once such misbehaving nodes participate within the route discovery section however refuse to forward the information packets, routing performance could also be degraded severely

In this paper, I've investigated the performance degra- dation caused by such misbehaving nodes in MANETs. I've analyzed performed to its performance. I've embedded some security aspects with 2ACK to envision confidentiality of the message by confirmative the first hash code with the hash code generated at the destination.

Our simulation results show that the 2ACK theme maintains up to ninety one packet delivery quantitative relation even once there square measure four-hundredth misbehaving nodes within the MANETs that I've studied. The regular DSR theme wills solely over a packet delivery quantitative relation of four-hundredth. The warning rate and routing overhead of the 2ACK theme square measure investigated in addition. One advantage of the 2ACK theme is its flexibility to manage overhead with the utilization of the R2ack parameter.

REFERENCES

1. E. Lorenzini, "Cooperation", in Proc. Sust. Coop. Multi-Hop Wirel. Netw., 2007 [Online]. Available: http://www.research.microsoft.com/enus/um/people/ratul/.../nsdi2005-catch.pdf
2. G. F. Mariasy, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation enforcement schemes for MANETs: a survey: re- search articles", in Wirel. Commun. Mobile Comput., vol. 6, iss. 3, pp. 319–332, 2006.
3. L. Tamilselvan and V. Sankaranarayanan, "Prevention of co- operative black hole attack in MANET", J. Netw., vol. 3, no. 5, pp. 13–20, 2008.
4. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing mis-behavior in MANETs", IEEE Trans. Mob. Comput., vol. 6, no. 5, pp. 536–550, 2007.
5. S. Dhanalakshmi and, M. Rajaram, "A reliable and secure frame- work for detection and isolation of malicious nodes in MANET", Int. J. Comp. Sci. Netw. Secur., vol. 8, no. 10, pp. 184–190, 2008.
6. D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Tal- pade, C. Ko, R. Balupari, C.-Y. Tseng, T. Bowen, K. Levitt, and J. Rowe, general cooperative intrusion detection architecture for MANETs", in Proc. 3rd IEEE Int. Inform. Assur. Worksh., College Park, USA, 2005, pp. 57–70.
7. W. Kozma Jr. and L. Lazos, "Reactive identification of misbehaviour in ad hoc networks based on random audits", 2008 [Online].