Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 7, July -2017

Improvement of Packet Dropping in MANETs by Using Acknowledge Based Approach

[1]Nikhil G. Wakode

[1]*M.E. Student*
[1]*Department of Computer Science & Engineering,*
[1]*Government College of Engineering, Aurangabad, India, 431005*

Abstract— *Main requirement in mobile ad hoc network (MANET) is to maintain the communication to all nodes and each node should amalgamate to each other. In the case of malicious nodes, it may create serious security issues, for the time of malicious nodes may collapse the routing process. In this text, defending the blackhole attack is the issued. This paper is used to solve packet drooping by using Temporally Ordered Routing Algorithm (TORA) routing by cooperative bait detection approach (CBDA) with malicious node detection algorithm. TORA referred the hybrid routing protocol and CBDA referred reactive and proactive routing mechanism. Malicious node detection algorithm indentifies the malicious nodes in the network. TORA based on concept of link reversal approach and CBDA implements a reverse tracing approach to achieve the desired goal. Simulation results have mentioned, TORA, existence of malicious nodes in TORA and securing malicious nodes in TORA by using CBDA with Malicious node detection algorithm in terms of packet delivery ratio, end-to-end delay, normalized routing overhead and throughput (taken as performance matrices).*

Index Terms— *Query (QUE), Update (UPD), TORA, Malicious node, Mobile ad hoc network (MANET), Cooperative baits detection approach (CBDA), TORA with malicious nodes, Secure TORA.*

I. INTRODUCTION

The mobile ad hoc network is spread as worldwide. It has been worked in many applications such as sensor network, commercial sector, military sector, tactical network, device network. It is mainly as, it does not consist any infrastructure. In MANET each node works as host and router. When node is transmitting data packets at that time nodes should cooperate to each other, also making wireless local network. These feature concern into the security issue of drawback. In precedence applications enforce some impulse on security of the routing, data traffic, network topology. In presence of malicious node in the network may derange the routing process.

In blackhole attack node relays data packet information to the destination by using shortest path, with the goal of objecting message. Malicious node lure all packets by using mould route reply packets to basely state that "sham" shortest way to the destination. Checking a trust based security solution in the network defending malicious nodes. It discards packets passed from it. In this paper, focus on improvement of packet dropping using TORA based routing technique.

TORA is a distributed routing algorithm based in MANET. There is no centralized control on a single node. TORA, initially behave as proactive routing protocols, because of starting nodes have routing table. Whenever the nodes does not in route o reach the destination then it starts route discovery and that time behave as reactive routing protocols. So every node, whenever wants to send a data they can send a data to every node, they run TORA routing algorithm to find out the route. In case of failure they maintain the route as well. TORA inculpates basic tasks.

1) Route creation
2) Route maintaining
3) Route erasing

In creation of route phase, a source node telecast a query packet (QUE) packet through the network. The intermediate nodes accept that request packets and broadcast to the other node to get destination node. When, the destination is found, then destination replies that update packet (UPD) through intermediate node to the source node to the reverse order by link reversal method. After route is discovered that time it will start the communication between source node and destination node. Another phase is route maintaining, in that source node wants to send data packets to given destination node. At certain times source send another data packets to given destination port because of route is maintained. If data packet is received to destination port means route is maintained otherwise algorithm is erased the route and searches the route to reach the destination address.

@IJAERD-2017, All rights Reserved

In this paper, CBDA with malicious node detection algorithm is suggested that capability flaw the malicious nodes that strive to pitch blackhole attack. In this approach, the intermediate node is handled as bait destination address to bait malicious node is sent reply RREP message and malicious nodes have been defended using reverse technique. Malicious node detection algorithm has identified malicious nodes in the network and mentioned record how many malicious nodes are working in the network and how are they.

II. RELATED WORK

In research work**,** number of mechanism has been taken into consideration to make certain security for the various attacks in MANET. To reduce the disregard of MANET in terms of packet drop, routing overhead, end-to-end delay, packets delivery, throughput, flow control.

Xiaoxue Lia et al. (2015) have proposed a thread model for smart meter. The smart meter are stated of being exposed to the possibility of being harmed physically in such way that hardware, firmware, design and implementation.

Jian Ming chang et al (2015) has proposed to resolve issue by mechanism of Dynamic Source Routing (DSR) which is referred to cooperative bait detection approach. The advantage of CBDA, It merges not only proactive but also reactive routing architecture. CBDA implements a reverse tracing technique to maintain the certain communication among source and destination through intermediate node. CBDA uses DSR, 2ACK, BFTR protocol in term of end-to-end delay, packet drop ratio, packet delivery ratio, routing overhead, throughput.

Adnan Nadeen et al. (2013) has proposed attack at network layer, such as eavesdropping, data modification, denial-of-service, compromised and sniffer attacks defending malicious node mechanism deal with this attacks.

Ziming Zhao et al. (2012) have proposed a risk aware response mechanism to identify the routing attacks. It is applied because number of nodes which isolate malicious node using binary isolation and also that to identify routing attacks in MANET.

III. PROPOSED APPROACH

Creation of Route in TORA:

In this TORA algorithm, the route creation between source node to destination node and also that it maintains routing tables for each period of time route table has updated when the network is not stabled. Initially source node broadcast UQE packets through the network and finding shortest path to reach destination in that number of copy QUE packets to be discarded when nodes already have QUE data request packet. When it reached to destination through intermediate node then destination node reply UPD data packets through intermediate nodes to the source node in way that route discovery is worked.

Route Maintaining in TORA:

TORA maintains the no. of route to reach the destination. Also that it maintains routing table of the all route. The route discovery mechanism is maintained route from source node to destination node. Source node has transmitted data packets to destination node through intermediate nodes. In that, source node wants to send another data packet to the same destination node. In that case source node sends the data packets to desired destination port from given route, it is already maintained. In the case of given route is broken that time TORA send data through another route to reach the destination address because of route maintaining mechanism.

Route Erasing in TORA:

In the case of route erasing, if the source node cannot be reached to destination port at that time TORA erases all routes and newly search the route to reach the destination port.

Malicious Node in TORA:

A malicious node is defined as node pursuing to impulse service to the node in the network. If trusted value if the destination node decrease with time to other node in the network. Malicious nodes, which reconstructs data packets before or after transmission called as malicious nodes. When malicious nodes have occurred in the network, then data packets has dropped. Then the malicious nodes are transmitting fake data packets in the network. It does not complete transmission to source node to destination node, when packets reaches to the malicious node that time malicious node dropped the data packet and transmission to be uncompleted.

@IJAERD-2017, All rights Reserved

In case of cooperative bait detection approach (CBDA). It consists of reverse tracing technique to achieve the goal. It contains three steps:

1. Initial bait step
2. Reverse tracing step
3. Shifted to reactive defense step

Initial bait step:

The goal of initial bait step phase is to tempt malicious node to send RREP by forwarding the bait RREQ' that has employing to post itself making shortest path to destination node that retard the packet were traveled. To attain this goal, initial bait step is designed to create the destination address of bait RREQ'.

The source node selects intermediate adjacent node within one hop count intermediate node and amalgamate with the node catching it's address as destination address of the bait RREQ'. When the baiting is done then it starts moving to another intermediate node and that bait would not change. The bait is animated and it sends bait RREQ' to other adjacent intermediate node by taking initial routing path. When malicious node is occurred that time it will start reverse tracing by TORA route discovery mechanism.

Reverse Tracing step:

The reverse tracing phase is worn to mark the performances of malicious nodes through the route reply to the RREQ' reply message. If malicious nodes has collected the RREQ' reply message. It will reply a fake RREP. The reverse tracing mechanism will be managed for node receiving RREP with the desire goal to infer the unsure path information and non permanent reliance area in the route. It should be highlighted that CBDA is not unable to note more than one malicious node when node send reply RREP.

Shifted to reactive defense step:

The initial bait step and reverse tracing step are proactive phase. After the TORA, route discovery process is started and the route is maintained. At the destination port, when the data packet is to be done by using malicious node detection algorithm. The malicious node detection algorithm has designed that packet delivery falls under proper destination node from the source node. In CBDA process, it should be observed that the malicious node as well as desired node information is obtained.

Malicious Node Detection Algorithm:

Step1. Select Source and Destination

Step2. Broadcast RREQ packet from source node

Step3. Search intermediate node and shortest path

Step4. If reply the RREP packet
It is destination
Else
Broadcast packet to other intermediate node
Step5. If packet drop
Malicious node
Else
Intermediate node, Go to Step 3
Step6. End

IV. PERFORMANCE EVALUATION

A. Simulation Parameters

The Network simulator 2 (version 2.32) is used to study the performance of CBDA and used IEEE 802.11 MAC with data rate 11 Mb/s. In simulation, malicious node detection algorithm is taken into consideration and certain parameter which is mentioned below in Table1.

@IJAERD-2017, All rights Reserved

Table1. Simulation Parameters

Parameter	Value
Application traffic	10 CBR
Transmission rate	4 packet/sec
Packet size	512 bytes
Pause time	0 sec
Maximum speed	10 sec
Simulation time	500 sec
No. of nodes	10, 20, 30, 40, 50
Malicious node	10%
Topology	700 m * 700 m

B. Performance matrix:

The performance matrix contains two sections. One is destination port and another is source port. In which destination port has contained receiving of data packets and source port has contained generation of data packets.

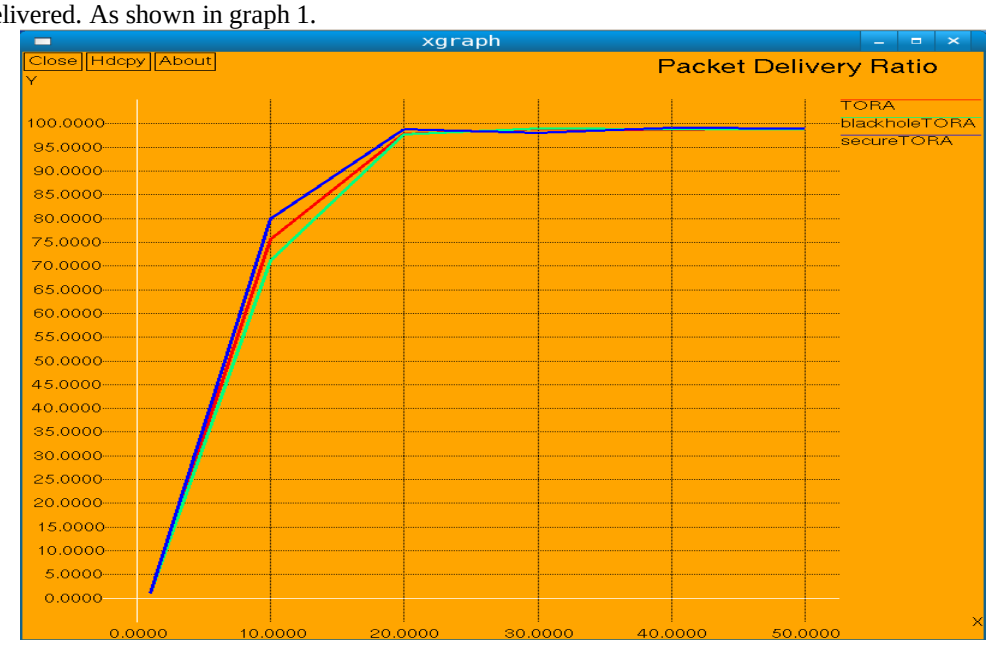
1) **Packet Delivery Ratio (PDR):** PDR is defined as the ratio of destination has received packets to the source level.

2) **End-to-End Delay:** This term is defined as at one's convenience for a packet to be mediated from source level to destination level.

3) **Normalised Routing Load:** It is stated that ratio of the count of routing control packets impart to the count of data impart.

Packet Delivery Ratio:

In packet delivery ratio, the comparison between TORA routing mechanism, malicious node with TORA routing mechanism and Secure TORA routing mechanism. Secure TORA routing mechanism means that using CBDA with malicious node detection algorithm with TORA routing mechanism. On the X-axis, no. of nodes and Y-axis, no. of data packets are delivered. As shown in graph 1.



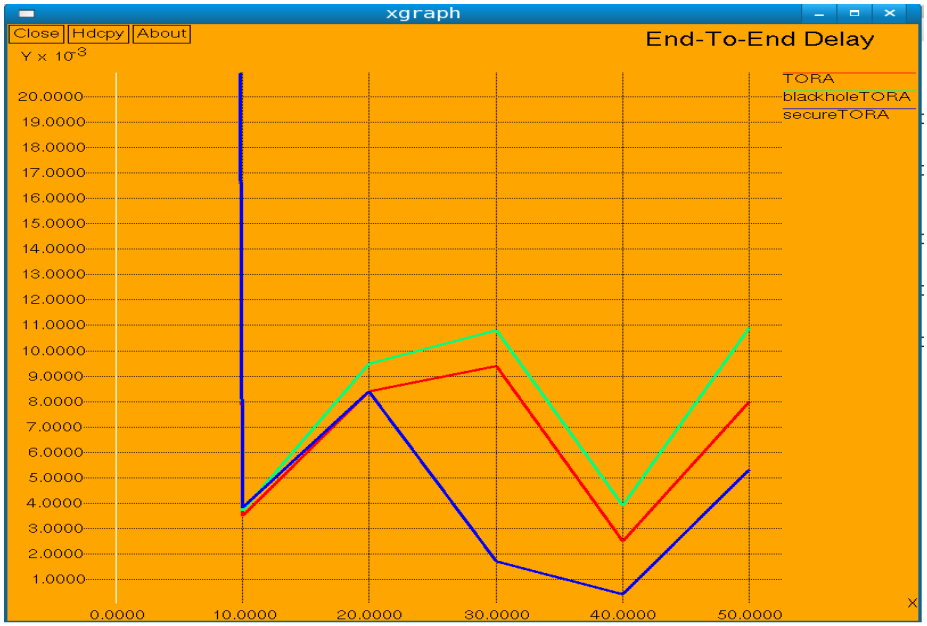
Graph1. Packet Delivery Ratio

End-to-End Delay:

In end-to-end delay, the comparison between TORA routing mechanism, malicious node with TORA routing mechanism and Secure TORA routing mechanism. Secure TORA routing mechanism means that using CBDA with

@IJAERD-2017, All rights Reserved

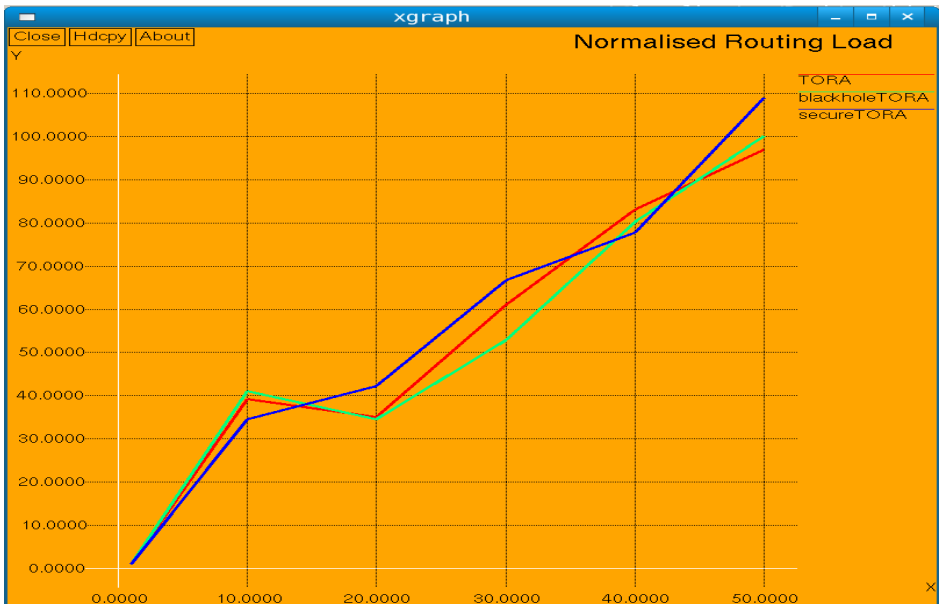
malicious node detection algorithm with TORA routing mechanism. On the X-axis, no. of nodes and Y-axis, time delay. As shown in graph 2.



Graph2. End-To-End Delay

Normalised Routing Load:

In normalised routing load, the comparison between TORA routing mechanism, malicious node with TORA routing mechanism and Secure TORA routing mechanism. Secure TORA routing mechanism means that using CBDA with malicious node detection algorithm with TORA routing mechanism. On the X-axis, no. of nodes and Y-axis, no. of control packets transmitted. As shown in graph 3.



Graph3. Normalised Routing Load

V. CONCLUSION

In this paper, proposed methodology is to improve packet dropping in MANET by using cooperative bait detection approach with malicious node detection algorithm. Presence of malicious nodes performance of packet delivery ratio, end-to-end delay, normalized routing overhead are decreased. By using cooperative bait detection approach and malicious node detection algorithm, the efficiency of packet delivery ratio, normalized routing and end-to-end delay are increased. Also those secure communications are performed in the network simulator. The results are carried out in NS2.

@IJAERD-2017, All rights Reserved

VI. ACKNOWLEDGMENT

The author wants to give thanks to the faculty members of Department of Computer Science and Engineering of Government College of Engineering, Aurangabad (MH), India for their support and guidance for research of this topic.

REFERENCES

[1] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in *Proc. 2nd Intl. Conf. Wireless Commun., VITAE*, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[2] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013).

[3] C. Chang, Y.Wang, and H. Chao, "An efficient Mesh-based core multicast routing protocol on MANETs," *J. Internet Technol.*, vol. 8, no. 2, pp. 229– 239, Apr. 2007.

[4] Xiaoxue Liu Peidong Zhu, Yan Zhang, and Kan Chen," A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure", IEEE TRANSACTIONS ON SMART GRID, VOL. 6, NO. 5, SEPTEMBER 2015.

[5] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai," Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE SYSTEMS JOURNAL, VOL. 9, NO. 1, MARCH 2015

[6] Adnan Nadeem, Michael P. Howarth," A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER 2013.

[7] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn and Ruoyu Wu , "Risk-Aware Mitigation for MANET Routing Attack IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO.MARCH/APRIL2012.

[8] B. Kannhavong, H. Nakayama, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE trans. Wireless Commun.*, vol. 14, no. 5, pp. 85–91, Oct. 2007.

[9] Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks" *in Proceedings of the 2nd International Conference on Intelligent Systems, Modeling and Simulation (ISMS'11)*, pp. 338-343, 2011.

[10] A.Rajaram and Dr. S. Palaniswami, "The Trust-Based MAC- Layer Security Protocol for Mobile Ad Hoc Networks", *In International Journal of Computer Science and Information Security (IJCSIS),*Vol 2. No. 2, pp. 400-408, 2010.

@IJAERD-2017, All rights Reserved