ISSN: 2455 - 9172

EIJO Journal of Engineering, Technology And Innovative Research (EIJO–JETIR)

Einstein International Journal Organization (EIJO)

Available Online at: www.eijo.in

Volume – 8, Issue –3 , May - June - 2023 , Page No. : 31 - 38

Packet Loss Avoidance and Trust-based Fine Grained Analysis Optimization and Generalization in MANET

[1]Arvind Kunwar, DR. K.N Modi University, Newai

[2]Aneesh Kumar Mishra, DR. K.N Modi University, Newai

Abstract

In MANETs, trust can be defined as to what extent a node can fulfil the expectations of another node. Packet loss detection and prevention is significant module of MANET security systems. In trust based method routing decisions are managed by an independent trust table. Traditional trust-based methods unsuccessful to detect the main underlying reasons of a malicious events. If MANET do not using fine-grained analysis method of packet drop in trust based method, the network may treat normal packet drop as malicious activity. It will misleads the MANET. Without fine-grained analysis the network may treat normal nodes as malicious and candisconnect from communication. It can degrade the network performance and malicious nodes remain undetected. We proposed a method which will improve the security in network by identifying the malicious nodes using improved fine grained packet analysis method. The method also improved the routing security using proposed algorithm. The system will improve the network performance and packet delivery ratio.

Keywords: MANET, Packet Loss Analysis, Malicious node, FGA, PDR

Introduction

Mobile Ad-Hoc Network (MANET)[1] is associate infrastructure less arrangement of mobile nodes which will randomly modification their geographic locations such these networks have dynamic topologies and random mobility with forced resources. Numerous inherent limitations, like totally distributed architecture and constantly varying topology, make MANET as vulnerable to a number of attacks by mischievous nodes. In MANET all nodes cooperation is necessary in order to make sure an appropriate functionality.

Some of examples of node attacks[2] are: (i)a node may drops data packets because of malicious behavior; (ii)a node doesn't take part in routing procedures in order to protect its energy and (iii) a node make available fake routing information to other nodes in order to interrupt the network.

To isolate and identify nodes which are non-cooperative in MANETs, an array of trust-based safety systems have been suggested. According to MANETs, trust can be well-defined as to what amount a node can accomplish the anticipations of another node. In trust-based systems, each node within the network be able to manage a sovereign trust table to store and compute the trust values of former nodes. Routing choices are then constructed on such calculated trust values.

Present trust-based systems fail to internment the real primary origins of an adversative event which may leads to several false positives through which validnodes are acknowledged malicious and to little detection rates for malevolent nodes. The motive for such deficiencies is that individual's trust-based safety systems assume that packet damages only get up due to mischievous actions by disobedient nodes. Conversely, packet damages in MANETs possibly will rise because of other adversative events, like congestion, wireless link transmission errors, and mobility[3]. Deprived of a

fine-grained investigation of packet damages in the trust building procedure, traditional systems may outcome in inaccurate trust assessments, specifically below high node mobility and high data rate.

Maximum present trust-based security arrangements for MANETs consider packet loss as a sign of probable attacks by means of malicious nodes. The packet loss possible reasons may be node mobility, queue overflow and interference. Recognizing the actual fundamental reason of a packet loss event is essential for any security scheme. The actual reason to find packet loss and malicious node fine grained analysis[4] is necessary. Because detection of innocent nodes as malicious nodes and without fine grained analysis the performance of MANET may degrade. And also malicious nodes may remain undetected without fine grained analysis. Consequently, methodologies are necessary that can appropriately recognize the mainreason for packet losses and can respond accordingly.

The rest of the paper is organized as follows.

Section 2 represents literature survey. Section 3 provides proposed work and algorithm. Section 4 provides the implementation details of the proposedwork. Section 5concludes the paper with a summary of the work and discussion of future research directions.

Literature survey

The author in [5] represent a system that is capable to appropriately recognize malicious nodes, by applying network parameters to decide whether packet losses are because to node mobility or queue overflows in MANETs. The author proposed FGA system for packetloss and the improvement of a wide-ranging trust model for mischievous node isolation and identification. The suggested FGA system is estimated in relations of performance metrics and efficiency under dissimilar network configurations and parameters. The experimental outcomes show that the proposed trust system accomplishes a noteworthy lessening in false positives degree and a rise in the rate of recognition of accurately mischievous nodes compared with normal non-FGA systems. FGA system inspects the reasons of data packet losses and provides information to the network about most possible reason of packet losses. The proposed model first recognize the main parameters for investigating the reason ofpacket losses in dissimilar aspects. The FGA system applied a number of dissimilar parameters like MAC layer data, queue data, and rate of link variations to summary the associations between nodes and nodes' neighbourhoods. The intention for applying local information for each node is to accomplish more perfect information and observation of network. Even though global information possibly will in some circumstances make available appropriate information, it is probable that false information delivered by the mischievous node can evade the safety mechanisms. In addition, as the FGA system necessitates information about the node neighbourhood, each node applied its personal local data to take a more informed result. The author present a method that is capable to appropriately recognize malevolent nodes[6], with the help of network parameters to conclude whether packet losses are because of queue overflows or node mobility in Adhoc. The authors proposed method for data packet loss and the improvement of a widespread trust system for malicious node identification and isolation. The proposed Fine-grained analysis method is estimated in terms of effectiveness and performance metrics under dissimilar network parameters and configurations. The author in [7] technique recommend a novel procedure to recognize malicious node affected by hole black attack and construct dimension estimations that are resilient to numerous compromised sensors even when

they conspire in the occurrence. The methodology tracked in this paper is based on dimensions investigation and its applicability depend on the supposition that the measurements are associated under unaffected environments, while negotiated measurements interrupt such connections. The drawbacks of the scheme[8] is that the dimensions encompass duplicate information. This will not sense irregular fluctuations in the spatial patterns.

The author in [9]provides information about routing security. It also provides detection of blackhole attack.One constraint of the projected method is that it workings based on a postulation that malevolent nodes do not effort as a group, even though this may occur in an actual condition. This paper does not provides group attacks problem. Node number, trust value generated during network initialization and threshold values are used to calculate confidence key. Confidence key is equal to product of threshold value, node value andtrust key. This confidence key value is used to validate the node.

D. Son et. al. 2005 [10] provides information about recommendation based trust model for MANET. It successfully provides details and differentiated the dishonest and honest recommendations. This algorithm will not work on blackhole and location and time based attacks. Initially all the required parameters, number of nodes, and threshold value for the network. The proposed algorithm will detect black hole based attacks in the network and informed to the network. If other nodes are authenticated nodes then select nodes forpath creation. Otherwise backup nodes are used to select different authenticated nodes from list.

Proposed Method

The steps in proposed work is as follows.

FGA scheme on subset of nodes. The extra parameters used are PDR, queue length, timestamp, increasing packet size.Protocol used is AODV, Trust-based security mechanism

Initially all the required parameters are provided input to the input as algorithm. The parameters are source node, number of nodes, destination node etc. All the threshold values are provided to the algorithm. Theconfidence key and trust key are used to authenticate the nodes in a network. Node number, trust value generated during network initialization and threshold values are used to calculate confidence key. If other nodes are authenticated nodes then select nodes forpath creation. Otherwise backup nodes are used to select different authenticated nodes from list. If node dropping packets at regular interval and performance is degraded below threshold value then black hole attack is identified in the network

Step 1: Start

Step 2: Fill mandatory information in RQ packet ofsender

Broadcast the RQ packet to construct route request andfind out route to the destination end

Step 3: The request is acknowledged by intermediarynode or destination node

If RQ received is identical thenThrow away the RQ

Else if fresh or restructured route is established then Next update the routing information entry for the source node

Build or update inverse route in the directionof the source node

End if Step 4:

If receiving node is one or the other the intermediary ortarget node with newer route then

Goto step 2

Else

Take the mandatory field values as of thereceived RQ

Update compulsory fields in the RQbeforehand broadcasting

Rebroadcast the RQ packet

End if Step 5:

If sending node is target node then

Increase the destination series number

End if

Fill RP packet with the mandatory columns

Send the RP packet on the inverse route in the directionof the source

Step 6: By means of an intermediate node on theinverse route or the source node

Record the mandatory column values from the receivedRP

Attachment of the corresponding documented valuesinto RP

If the neighbor directing RP is striking as blacklistedthen

Throw away the RP

Else if Fresh and restructured route is found then Update the transmitting table record for the destination nodeEnd if

If receiving node is the main source node thenReject the RP

Direct the data through the forward directionif the route is newer and the subsequent hop is reliable

Else

Forward the RP packet on the inverse route inthe direction of the source node

End if

Step 7: Update trust

For neighbor information entry do Authenticate the presence of attackinformation form neighbor

Estimate trust value of the neighbor nodeIf the neighbor follows attack information then Identify the node as mistrusted node

Else if the neighbor doesn't have information of attackvalue, and suggested as trusted node then

Identify the node as trusted node

End if End for

For routing information entry do

Discover the information of the subsequenthop from the neighbor information

If the subsequent hop is found to be disbelieved in theneighbor information then

Start a local route finding process to find out analternative route to the destination

End if

End for

Step 8: Belief recommendation

Create the vacant blacklist for reference purposeFor each neighbor information entry do

If the neighbor is identified as disbelievednode then

Supplement the neighbor identity into the blacklistEnd if

End for

Step 9: Integrate the blacklist into the HELLO datapacket

And broadcast the HELLO data packet as of theneighbors

Take HELLO data packet from the neighbor

If the neighbor directing the HELLO data packet istrusted then

Take the blacklist from the HELLO data packetFor each information in the blacklist do

Discover the equivalent information in theneighbor route table

If the neighbor information occurs then Set reference value as disbelieved for the neighbor

End if

End for

Step 10: End

Initially all the mandatory information is filled in the request packet RQ of the source node. The requestpacket RQ is then broadcast to construct route request and find out route to the destination end. The request is acknowledged by intermediary node or destination node. If received request is identical then simply throw away the RQ. If received request is fresh or restructured route is established then next update the routing information entry for the source node and buildor update inverse route in the direction of the source node.

The next step is to check the information for receiving node. If receiving node is one or the other the intermediary or target node with newer route then again all the mandatory information is filled in the request packet RQ of the source node otherwise take the mandatory field values as of the received RQ update compulsory fields in the RQ beforehand broadcasting and again rebroadcast the RQ packet.

The next step is to check if sending node is target node.If sending node is target node then increase the destination series number. The next step is again fill RP packet with the mandatory columns and unicast the RP packet on the inverse route in the direction of the source. By means of an intermediate node on the inverse route or the source node record the mandatory column values from the received RP and attachment of the corresponding documented values into RP. If the neighbor directing RP is striking as blacklisted then throw away the RP. Else if Fresh and restructured routeis found then update the transmitting table record for the destination node.

If receiving node is the main source node then reject the RP direct the data through the forward direction if the route is newer and the subsequent hop is reliable else forward the RP packet on the inverse route in the direction of the source node. The next step is to update trust. For each neighbor information entry do authenticate the presence of attack information form neighbor. Estimate trust value of the neighbor node if the neighbor follows attack information then identify the node as mistrusted node. Else if the neighbor doesn't have information of attack value, and suggested as trusted node then identify the node astrusted node.Next step is belief recommendation in proposed algorithm. Create the vacant blacklist for reference purpose for each neighbor information entry do the subsequent step if the neighbor is identified as disbelieved node then supplement the neighbor identity into the blacklist. Next step is to integrate the

blacklist into the hello data packet and broadcast the hello data packet as of the neighbors take hello data packet from the neighbor. If the neighbor directing the HELLO data packet is trusted then take the blacklist from the hello data packet for each information in the blacklist do the following step and discover the equivalent information in the neighbor route table if the neighbor information occurs then set reference value as disbelieved for the neighbor. The proposed algorithm also increases performance and the data delivery ratio of the network.

Implementation

The experiment is performed in PIV 2.4 GHz machine with 4GB RAM. Network Simulator 2 simulator platform is applied for implementation of recommended algorithm.

Table 1. Simulation parameters

Parameter	Value
MAC protocol	802.11
Traffic type	CBR-UDP
RP	AODV
Initial energy	0.5 Joule
No of nodes	50
Packet size	512 bits/ sec
Freq. range	5 GHz
Rece. power	0.01 watts
Tx. power	0.02 watts
Simulation area	1500 x 1500
Mobility model	Random way point
Max mobility	5m/sec to 25m/sec
% of malicious	0% to 50%
Simulation time	200 to 1000 sec
No of connect	10
Comm. range	250m
Channel b/w	2 Mbps

Table 2 Secure key generation during data transmission

Sn.	Node	Secure Key Value
1	Source (1)	1369634280
2	Destination (0)	1369634280
3	2	1369634280
4	15	1369634280
5	18	1369634280

The table 2 represents node number with secure key during data transmission. This trust key is used as secure key and authentication of node.

We have assigned initial belief value to each node which helps to find authenticate neighbors. The components of our proposed model are trust value, recommended trusted neighbors, and secure path. The threshold data value is measured as 0.9. The confidence key is designed as node * trust value *threshold value.

Suppose we have node 20 to check for authentication then its trust value is calculated according to the threshold value as

Confidence value = 0.9 * 20 * 1462252574

= 26320546332.0

The table below shows the belief node, trust value and confidence value of the network.

Table 3: Trust and confidence value

Node	Trust Value	Confidence Value
1	1462252574	1316027316.6
5	1462252574	6580136583.0
8	1462252574	10528218532.8
14	1462252574	18424382432.4
16	1462252574	21056437065.6

Table 4 Energy consumption analysis

Detect (Avg. energy consumption / No of nodes)	Prevent (Avg. energy consumption / No of nodes)	Attack (Avg. energy consumption /No of nodes)
0.5/25	0.5/25	0.6/25
0.78/50	0.60/50	1.1/50
0.96/75	0.63/75	1.5/75
1.2/100	0.68/100	1.8/100

As represented in table as attack increases in the network the energy consumption also increases. But after prevent scheme energy consumption decreases and system throughput also increases.

Conclusions

Traditional trust-based methods unsuccessful to detect the main underlying reasons of a malicious events. Maximum present trust-based security arrangements for MANETs consider packet loss as a sign of probable attacks by means of malicious nodes. The packet loss possible reasons may be node mobility, queue overflow and interference. Packet loss detection, reaction and report to the MANET is a significant factor of any widespread safety solution. Comprehensive examination and analysis of data packet are necessary to discover the actual reason of the packet loss. Real time applications in MANET require certain QoS features, such as minimal end to end info packet interval and acceptable data loss. The trustworthiness of distributing data packets from end to end by means of multi-system intermediary nodes is a remarkable difficulty in the mobile Adhoc network. The proposed algorithm which will increase the security in MANET by identifying the malicious nodes with the help of improved fine grained packet analysis method. The algorithm may also increase the security in routing. The system will improve the network performance and packet delivery ratio.

References

1. T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for AdHoc network research," Wireless Commun. Mobile Comput. Special Issue Mobile Ad Hoc Netw.: Res., Trends, Appl., vol. 2, no. 5, pp. 483–502, Aug. 2002.
2. R. Korsnes, K. Ovsthus, F. Y. Li, L. Landmark, and O. Kure, "Link lifetime prediction for optimal routing in mobile ad hoc networks," in Proc. MILCOM, Oct. 17–20, 2005, vol. 2, pp. 1245–1251.
3. M. Karthik and P. Senthilbabu, "PESR protocol for predicting route lifetime in mobile ad hoc networks," in Proc. ICON3C, 2012, pp. 22–27.
4. A. Kumar, S. Jophin, M. S. Sheethal, and P. Philip, "Optimal route life time prediction of dynamic mobile nodes in manets," in Proc. Adv. Intell. Syst. Comput., 2012, vol. 167, pp. 507–517.
5. Elisa Bertino, Daniele Midi, Muhammad Saleen Khan, Majid Iqbal Khan, " Fine Grained Analysis of Packet Loss in MANET", IEEE, 2017, pp. 7798-7807.
6. Yuxin Liu, Mianxiong Dong, Kaoru Ota, and Anfeng Liu, ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 9, pp-2013-2018,SEPTEMBER 2016,
7. N. Leone et al., "The DLV system for knowledge representation and reasoning," ACM Trans. Comput. Logic, vol. 7, no. 3, pp. 499–562, Jul. 2006.
8. N. Ramanathan et al., "Sympathy for the sensor network debugger," in Proc. ACM SenSys, San Diego, CA, USA, 2005, pp. 255–267.
9. A. Cerpa, J. L. Wong, L. Kuang, M. Potkonjak, and D. Estrin, "Statistical model of lossy links in wireless sensor networks," in Proc. IEEE IPSN, 2005, pp. 81– 88.
10. D. Son, B. Krishnamachari, and J. Heidemann, "Experimental analysis of concurrent packet transmissions in low-power wireless networks," in Proc. ACM SenSys, San Diego, CA, USA, 2005, pp. 237–250.