An Implementation of Residual Processing Among Nodes for Malicious Detection in Manets

[1] Yerra Aswanth, [2] Priyanka Kumari Bhansali
[1]M.Tech Scholar, Department of Computer Science and System Engineering,
Andhra University College of Engineering (A), Visakhapatnam, AP, India.
[2]Department of Computer Science and System Engineering,
Andhra University College of Engineering (A), Visakhapatnam, AP, India

Abstract: In mobile ad hoc networks (MANETs), data items can be retrieved effectively by using top-k query processing method. The environment which contains malicious nodes cannot provide an accurate result. This project assumes that the malicious node tries to attempt an attack called data replacement attack in which the necessary data sets are replaced by unnecessary data sets. The proposed work includes node grouping method in top-k query processing for detecting the malicious node. The query processing in mobile ad hoc network (MANETs) is optimized using top K-query concepts but this process in affected by the presence of malicious nodes in the environment where it may induce unrelated information. The presence of false date will not let to produce accurate result during query processing. The accuracy of the query result can be maintained by forwarding the data sets along multiple routes and based on the information attached to the reply message the query-issuing node can detect the attack. By exchanging the message, single malicious node can be identified. To identify multiple malicious nodes, it's necessary to share the information of identified malicious node to other nodes. In this method, nodes are grouped based on the similarity of the identified malicious node. Simulation experiments are conducted by using a network simulator, NS2, to verify that this method provides high accuracy and identifies multiple malicious nodes. In flexible imprompt frameworks (MANETs), it is capable to recuperate data things using top-k inquiry. In any case, exact outcomes may not be acquired in circumstances when malevolent hubs are accessible. In this project, we expect that malignant nodes attempt to supplant key data things with trivial ones (we call these data substitution assaults), and propose methods for top-k request get ready and pernicious node recognizable proof considering node assembling in MANETs. In the wake of recognizing attacks, the question issuing hub tries to perceive the malignant hubs through message exchanges with various hubs. The proposed method detects these attacks by using score values in top k query processing, in which nodes reply with data items and their score value are used to identify the data replacement attack in network.

Index Terms **– Mobile ad hoc networks, query processing, routing, traffic, data replacement attack, node grouping.**

I. INTRODUCTION

The mobile ad hoc network (MANET) is fewer infrastructures, decentralized and self configuring network. This is constructed by using the mobile nodes which are linked by wireless. Every individual mobile node in medium take action as a router and the nodes can be in touch with each other by inter-changing the information packets. Yet if initiator and target mobile nodes are not in the communication range, the information packets can be forwarded to the target node through the in-between nodes which exists among the two mobile nodes.[1]Multiple hops are necessary for a node to communicate with further node across the network. As of late, there has been an expanding enthusiasm for portable ad hoc system (MANET), which is built by as it were portable nodes. Since such self-circulated systems don't require previous base stations, they are relied upon to apply to different circumstances, for example, military issues and safeguard work in fiasco destinations. In MANETs, since every node has poor assets (i.e., the correspondence transfer speed and the battery life of versatile nodes are restricted), it is powerful to recover just the vital

information things utilizing top-k inquiry, in which information things are requested by specific characteristic score, and the question issuing node gains the information things with k most noteworthy scores in the system (the worldwide top-k result).The mobility in the network is high since the mobile nodes can move separately in any direction[2]. Owing to this, the link gets detached and the network topology changes quickly. Because of these dynamic activities, more routing protocols like proactive, reactive and hybrid are anticipated for MANET. Each mobile node has poor communication bandwidth and limited battery life span for data transmission.[3] A self-configuring and infrastructure- less mobile node with wireless link is called mobile ad hoc network. Each node can move independently and capable of routing traffic to other nodes in the network and these network don't have fixed infrastructure. To route the packet each node have to maintain the routing information and it has to be updated when the topology changes. In a MANET, nodes with in communication range can communicate directly with other node, if a node is outside the communication range it has to relay on some other nodes to forward the date. The implementation of MANETs is more relabel because no infrastructure is needed, the network can be deployed in emergency situation. Due to technology improvement MANET enters the area like distribute computing, gaming etc. The mobile ad hoc network has gained momentum recently due the nature of self-distribution of nodes without a base station[4.5,6]. In MANETs, each node has limited resource like communication bandwidth, batter life so they depend on other nodes for effective query processing. The nodes will use a top-k query processing method to get the knowledge of the entire network. A node will issue a query this query will moves form one node to another node based on the routing algorithm, and each node will contribute their answer and the items are ordered according to their attribute score and the query-issuing node will get the date with the k highest score in the network. In this environment some node will be a malicious tries to confuse and disrupt the normal operation of the network.. This paper, discuss about the procedure of top-k query and the methodologies proposed for reducing traffic and providing high accuracy of query results. The traffic in the medium will be high when enormous amount of data packets are transmitted. To stay away from the unnecessary traffic, the node retrieves only the required data packets. For this reason, a technique called top-k query is proposed. It is efficient to retrieve only essential data items in the huge amount of data items[7]. At this time, the data items are arranged by the scores of a particular attribute. A node which retrieves the data items is query-issuing node. This node floods a query note to every other node in the network. All mobile node transmits its data items with k maximum score (local top-k result) after getting the query message. The rest of this paper is prepared as follows: Section II deals with related works of top-k query

II. RELATED WORKS

In MANET, secure routing protocols protect against attacks and false data. In these protocols data transmission from source to destination occurs in multiple routes [15], [8], [11] and public keys are symmetric keys are used for data encryption [6], [9], [13]. In [15], the authors proposed a method where every sensor nodes forwards data items using Message Authenticate Code (MAC). MAC uses symmetric key for encryption. Whenever the node receives a message, it checks the validity of message. Even if the information encrypted data replacement attack cannot be avoided. In [11], authors proposed a method in which multiple routes are determined. The route request messages are encrypted using hash functions. In ad hoc networks [3], to obtain only the needed data items effectively each mobile node retrieves data items using a top-k query. In order to reduce the traffic with high accuracy of the query result, each node will send a histogram data [4] based on the query to query issuing node with this histogram it's easy to find the highest score value. A routing table based method is proposed in [5] to achieve high accuracy in query processing using top-k query.

The top -k query processing is performed in two phase[6] in phase one the query issuing node will collect all the query result and in second phase it will find out the result with highest score based on threshold calculation. In two-tier sensor network [7] master slave architecture is used. In which the master node collects data from sensor node and answers the query from the network owner in this method the master node should be a trusted node.

Top-k query is effectively used in the field of distributed and database systems to retrieve only the necessary data items from huge amount of data. In [1], [2], [4] and [10], authors proposed methods which adapts to mobility, provides high accuracy and reduces congestion. In [6], authors proposed secured query processing method in a network which contains malicious node. In [5], a method proposed to detect false data injection attack in which new and false data are generated by malicious node.

In [3], [7], [12] and [14], methods for many reputation systems are proposed. In [19] and [20], each mobile node manages the neighboring nodes reputation values. By analyzing the messages of neighbor node, each node determines the reputation value. In [17] and [18], authors proposed a method in reputation system which is against the false notification attack. This method exchanges a cryptographic key between sender and receiver in advance. Also, sends their ID with past and present reputation scores in encrypted form. The receiver node can decode and confirm the received reputation scores. So that false reputation scores can discard

III. PROPOSED METHOD

Network Creation

The Network is constructed with 60 mobile nodes without any base station as self-distributed nodes. Each node is assigned with a unique identification number and mobility pattern is random. The node can exchange data packets and control packets as defined by the protocol.

System Model

The network consists of mobile node is represented by N= {N1,N2,…..Nn} where n is the total number of nodes in the network and they are identified using the identification number NID={NID1,NID2,..NIDm}, Where m=n. The data in the network is denoted as D={D1,D2,…Dk}, where k is the total number of data and each data is identified by using data identifier Di, where i=k. The algorithm works in distributed environment so each node has to exchange more information with the nearby node so they exchange data packet frequently so to avoid intermediate nodes not to modify the data content public key encryption method is used. Each node knows the public key of other nodes so data are send by encrypting with the public key of the receiving node. In order to reduce the computation the query message are not encrypted.

Data Replacement Attack

The node in the network can generate a query and send it to the all the nodes to get a desired value. Let us assume a node need the person detail with a particular blood group with high blood pressure, low vision, this requirement is generated as query and propagated towards the network. Let us consider Mr be the query issuing node and Mq be the node that replay for the query with its own score value this is the normal situation, the case will not remain for long time. In some situation a malicious node may capture the node and induce its own low score value to make the aggregation to be invalid. The query form query issuing node have a query id and the id of the query issuing node (Qid, Nid) the query goes to nearby node and this node will include its score value and its identification (SVi,, Nid).There will be two list one is to store the replay Score Value List (SVL) and the second is Replay Path Value (RPV) which store the path of the query propagation message or replay message. The query will take multiple path in the network.

Top-k Query Processing

1. Query forwarding and replying

First, the query issuing nodes Mq floods query message to entire medium. It consists of query-issuing node identifier (Q-I_ID), query identifier (Q_ID), number of requested data (k), condition of query and the list of nodes in the path (Q_path).Mp sets waiting time (WT) in (1) for reply messages. In Algorithm Forwarding Query, hopCount denote number of hops to query issuing node.

WT= (maxhop - maxcount) . Twait (1)

When receiver node Mr receives query it stores the sender node ID and query path. In Algorithm Replying Query, when Mr needs to send reply message (RM), it selects the least hop count neighbor node from the information stored in forwarding list route (RM_FR).

Algorithm: Forwarding Query

- ✓ If Mr receives query for first time then
- ✓ Store Q_path and hopcount as parent path
- ✓ Store nodeID in Q_path as parent
- ✓ Set WT for replying messages
- ✓ Send query to neighbor nodeID
- ✓ Else
- ✓ Store Q_path and hopcount as neighbor path
- ✓ Store nodeID in Q-path as neighbor
- ✓ End if

2. Link Disconnection

In MANETs, topology of network changes frequently due to high mobility. When a node Mr tries to forward a reply message to neighbor node and link gets disconnected, it results in decreasing the accuracy of query result. To overcome this problem, whenever a node sends reply message it waits for the acknowledgement ACK from the sender node. When Mr doesnot receives ACK from parent node it detects the disconnection in radio link. Then, Mr sends data items through another neighbor node which has least hop count.

Algorithm: Replying Query

- ✓ For each neighbor do
- ✓ If hopCount of neighbor is minimum then
- ✓ Insert Neighbor as Destination
- ✓ End if
- ✓ End for
- ✓ Add local result to RM
- ✓ For i=0 to 1 do
- ✓ If i=0 then
- ✓ Add (Mr,parent ID) to RM_FR and send RM to parent ID
- ✓ Else if i=1 then
- ✓ Add (Mr,Destination) to RM_FR and send RM to Destination
- ✓ End if
- ✓ End for

Attack Detection

After receiving all reply messages, the query issuing node Mp detects DRA. In Algorithm Detection of Attack, T-k result denotes highest scores k. RM_Data and RM_FR denotes data list and forwarding route respectively. Sendroute denotes set of node

identifiers. A node can detect DRA when data items in T_k included in Sendroute but not included in RM_Data. To identify malicious node, query issuing node narrows down the candidates of malicious node in Sendroute. Miss T_k result denotes replaced data. If number of candidate is one, query node identifies this as malicious node. If number of candidates is more than one, an inquiry message M_INQ sends to other nodes. By reply message for inquiry query the malicious node candidate can be identified.

Algorithm: Detection of Attack

- ✓ If hop count to candidate = 1 then
- ✓ Return candidate as malicious node
- ✓ Else if hop count to candidate is > 1 then
- ✓ Send M_INQ to Mdes
- ✓ End if
- ✓ If Mdes receives M_INQ then
- ✓ Send M_Rep send by Candidate[i] to Mp
- ✓ End if
- ✓ If Mp receives M_REP then
- ✓ If scores includes in scores of Miss T_k result then
- ✓ Return candidate [i-1]
- ✓ End if
- ✓ End if

Global Identification

Each mobile node forms groups in medium based on the conventional information in notification messages. In Algorithm Node Grouping, sim(x,y) denotes resemblance of scores between Mx and My. Grp and G_CAN represent groups and candidates of groups respectively. denotes fth group of Grp. $_h$ denotes node in . First, each mobile node calculates similarity of malicious nodes based on received messages. Cosine similarity made in order to decrease the power of differences in recognized malicious node. After node grouping, a few groups may include both normal and malicious nodes. As a result, node performs cleaning in every group to eliminate contradiction. Following that, node identifying one more node which is identified by less than a certain integer of nodes in same group, is also removed from group

Algorithm: Node Grouping

- ✓ For each x ϵ n do
- ✓ For each y ϵ n do
- ✓ sim(x,y) = cos(x,y) = . /| || |
- ✓ End for
- ✓ End for
- ✓ For each x ϵ n do
- ✓ For each y ϵ n do
- ✓ If M_CAN = ø and sim(x,y) >= ø then
- ✓ insert Mx, My into G_Can
- ✓ Else if M_CAN ≠ ø and { ∀ ∈ M_CAN, sim(z,y) ≥ } then
- ✓ Insert Mx into G_Can
- ✓ End if
- ✓ End for
- ✓ For each Grp do
- ✓ For each $_h$ in do

- ✓ If $_h$ identifies node include in then
- ✓ Eliminate $_h$ from
- ✓ End if
- ✓ End for
- ✓ End for
- ✓ End for

IV. SIMULATION EXPERIMENT

This section deals with the results of simulation experiments conducted using the network simulator NS2. By using random waypoint model nodes are created and initial position determined randomly. The data items from each mobile node are transmitted using IEEE 802.11b device.

Performance Metrics:

The following three performance metrics are measured in this simulation.

II. Accuracy of query result: It represents the average ratio of data items provided in the top-k result acquired by query-issuing node.

III. Traffic: It represents the total volume of traffic taken for processing the query and for detecting the malicious node.

IV. Malicious Node Identification Ratio: It represents the average ratio of the number of identified malicious node using node grouping technique.

Simulation Results:

Figure.1 shows the accuracy of query result acquired by query-issuing node. The X-axis denotes the number of requested data items and Y-axis denotes the accuracy. The proposed top-k query method increases the accuracy even when the number of requested data items is large. Figure.2 shows the traffic occurred when query results are forwarded in multiple routes. The X-axis denotes the number of requested data items and Y-axis denotes the traffic. Figure.3 shows the malicious node identification ratio that represents maximum number of identified malicious node by issuing less number of queries. The X-axis denotes the query issuing time and misidentification.

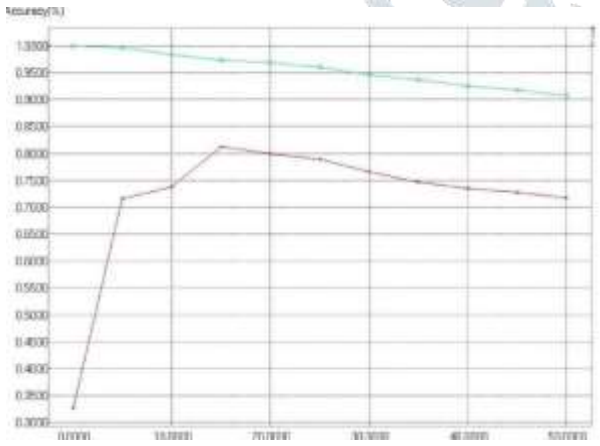

Figure 1: Accuracy of Query Result

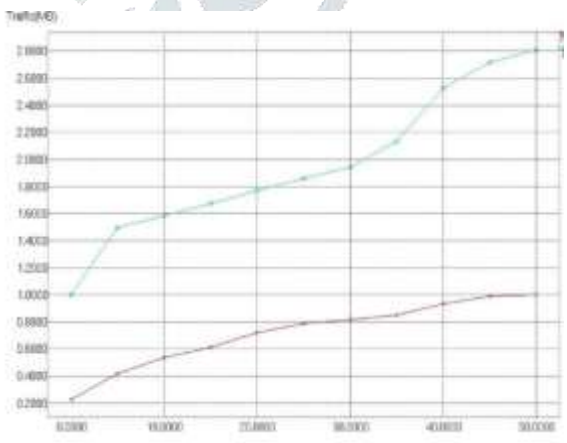

Figure 2: Traffic

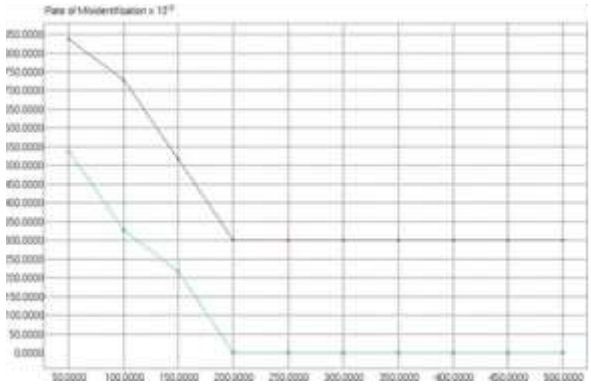

Figure 3: Malicious node identification ratio

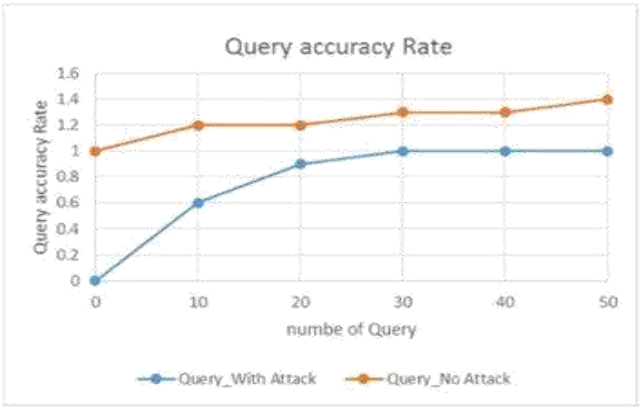

Figure 4. Query Result Accuracy

V. CONCLUSION

we proposed node grouping methods for top-k query processing to identify multiple malicious node. To maintain high accuracy of reply message and to detect data replacement attack, k data items are transmitted along multiple routes. When query issuing node detects an attack it narrows down the malicious node candidates. Then malicious node identified by exchanging message with other nodes. Single query is not sufficient to identify multiple malicious nodes. So the information about identified malicious node shared with other nodes in network. In node grouping technique, nodes are divided into some group based on the similarity of the received information. Then, malicious nodes are identified based on group information. Since reply messages are transmitted along multiple routes, traffic in the network gets high. As a part of future work, a method can be proposed to reduce traffic and to provide message authentication.The proposed work is designed to provide secure data sharing among the nodes present in Mobile Ad-hoc Networks. As per the previous work the query-issuing node was not able to identify attacker node if present in large numbers

FUTURE WORK:

A wireless sensor Network consists of spatially dispersed self-directed sensors to monitor the environment conditions. In probabilistic Top-k, a new approach such as Expected ranking method is used to get accurate result in finding Top-k results and as well as accurate probability. For inter cluster processing three algorithm is used namely Sufficient-set based, Necessary-set based and Boundary based algorithm. For reducing transmission cost adaptive algorithm is used and this gives the efficient result in the bounded rounds of communication. This gives least transmission cost and not exceeds two rounds of communication.

REFERENCES

[1] D. Amagata, Y. Sasaki, T. Hara, and S. Nishio, ``A robust routing method for top-k queries in mobile ad hoc networks," in Proc. MDM, Jun. 2013, pp. 251fi256.

[2] W.-T. Balke, W. Nejdl, W. Siberski, and U. Thaden, ``Progressive distributed top-k retrieval in peer-to-peer networks," in Proc. ICDE, Apr. 2005, pp. 174fi185.

[3] S. Buchegger and J.-Y. Le Boudec, ``Performance analysis of the CONFIDANT protocol," in Proc. MobiHoc, 2002, pp. 226fi236.

[4] T. Camp, J. Boleng, and V. Davies, ``A survey of mobility models for ad hoc network research," Wireless Commun. Mobile Comput., vol. 2, no. 5, pp. 483fi502, Sep. 2002.

[5] B. Chen, W. Liang, R. Zhou, and J. X. Yu, ``Energy-efficient top-k query processing in wireless sensor networks," in Proc. CIKM, 2010, pp. 329fi338.

[6] H. Chan, A. Perrig, and D. Song, ``Secure hierarchical in-network aggregation in sensor networks," in Proc. CCS, 2006, pp. 278fi287.

[7] S. Chen, Y. Zhang, Q. Liu, and J. Feng, ``Dealing with dishonest recom- mendation: The trials in reputation management court," Ad Hoc Netw., vol. 10, no. 8, pp. 1603fi1618, Nov. 2012. [8] P. Dewan and P. Dasgupta, ``P2P reputation management using distributed identities and decentralized recommendation chains," IEEE Trans. Knowl. Data Eng., vol. 22, no. 7, pp. 1000fi1013, Jul. 2010.

[9] N. C. Fernandes, M. D. D. Moreira, and O. C. M. B. Duarte, ``A self- organized mechanism for thwarting malicious access in ad hoc networks," in Proc. INFOCOM, 2010, pp. 266fi270.

[10] R. Hagihara, M. Shinohara, T. Hara, and S. Nishio, ``A message processing method for top-k query for traffic reduction in ad hoc networks," in Proc. MDM, May 2009, pp. 11fi20.

[11] Y.-C. Hu, A. Perrig, and D. B. Johnson, ``Ariadne: A secure on-demand routing protocol for ad hoc networks," in Proc. MobiCom, 2002, pp. 12fi23.

[12] Y.-C. Hu, D. B. Johnson, and A. Perrig, ``SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," Ad Hoc Netw., vol. 1, no. 1, pp. 175fi192, Jul. 2003.

[13] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, ``The Eigentrust algorithm for reputation management in P2P networks," in Proc. WWW, 2003, pp. 640fi651.

[14] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, ``An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536fi550, May 2007.

[15] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, ``Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method," Int. J. Netw. Secur., vol. 5, no. 3, pp. 338fi346, 2007.