International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

# Disaster Management Using Top-K Query Processing And DRA Identification in MANETs

**Thulasi Rajan.K[1]**

[1,] *Department of Computer Sci. & Engg, Thejus Engineering College, Vellarakkad, Thrissur, Kerala, India*

---

**Abstract –** *Top-k query processing can be used in MANETs for efficiently retrieve top-k data items. The data items in each node are prioritized by an attribute value. The top-k values are calculating by this score value. A malicious node can replace the high priority data with its own low prioritized data; this is called as data replacement attack (DRA). This paper proposes a method to detect DRA and to identify the malicious node. It ensures an efficient top-k result for the queries. Top-k query processing can be used in disaster management where the details of the victims want to be collected for rescue operations. Details of victims can be grouped based on their priority values for the rescue operations. Also the locations of victims can be tracked using this method.*

***Key Words*: Disaster management, Top-k query processing, Data replacement attack, Grouping, Location identification.**

## 1. INTRODUCTION

Among recent advances in radio communication and mobile technologies mobile adhoc network has an increasing interest.MANET is a collection of mobile nodes which has no fixed infrastructure. It has no centralized control so it can move and communicate rapidly. The nodes in MANET can be host or router, the nodes plays the role of both for data transmission. Multi-hop routing is a major feature of MANET even if two nodes are not in communication range they can perform their transmissions by forwarding the data packets through the neighbour nodes. The intermediate nodes are used to route the packet to destination node. Because of these features MANET can be used for a wide range of real time applications such as rescue operations in disaster areas. The nodes of MANET are mobile it has only limited resources for their working. In the case of top-k query retrieval the query issuing node wants the data items having top-k priority scores, so each node wants to communicate each other to make the decisions of their data score priorities. The communications for the top-k results decreases the energy of the nodes. So the data retrieval should be done efficiently in minimum resources. So an efficient top-k query processing method is needed for this. If there are malicious nodes in the network they can affect the query retrieval, it will decrease the efficiency of the query result.

A type of attack called data replacement attack (DRA)[1] can be done by the malicious nodes in the network. Malicious node replaces the details of the people who need urgent rescue operations. Malicious node replaces the highest values of data scores with its own lower values, this will return an in efficient query result to query issuing node. The proper rescue operations will disrupt here. So the malicious nodes of the network want to be identified for making the query result an accurate one. The peoples in disaster areas will be in critical rescue conditions or in average or low prioritised conditions, so the grouping of each nodes based on the severity conditions can make the rescue operations more fast and easy. If the rescue workers can immediately locate positions of the nodes who need immediate rescue operations will improve the efficiency in rescue operations.

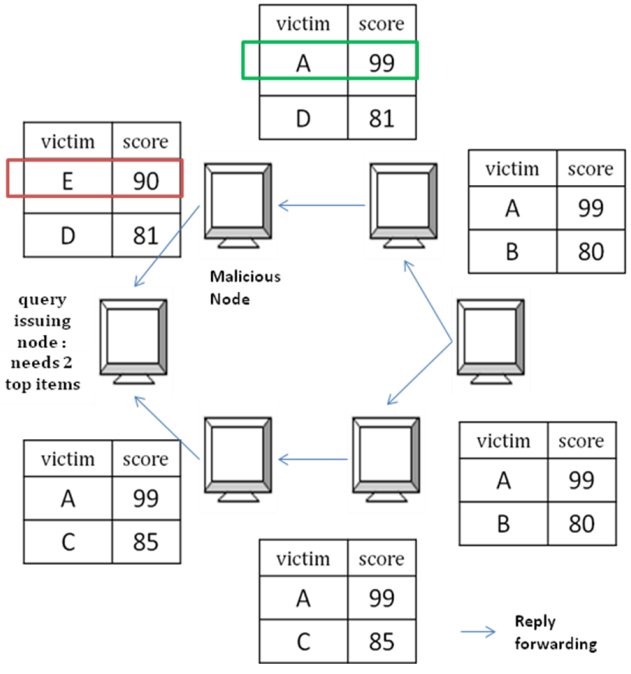


**Fig -1**: Data Replacement Attack

In Fig-1 The malicious node replaces the high scored data item A-99 with its own low scored item E-90.

## 2. LITERATURE REVIEW

[2] A message processing method which reduces un necessary data transmissions and it also finds an alternative path if link disconnection occurs. Each node estimates high scores and set standard score. This score is used for query transmission and retrieval. It shares the scores to neighbors for the updates.

[3] A robust routing method by keeping high accurate query results. It multicast the query message to nodes in the routing table. It uses multipath transmission of query messages, each node hold a routing table and knows the successor to forward the query. It Make efficient query retrieval by finding other paths in the cases of link disconnections.

[4] Malicious node identification method, which has three phases for the malicious node identification. First phase uses an end to end acknowledgement scheme for packet transmissions. Second phase is SACK, it checks the malicious node between 3 nodes. Third phase is MRA, it deals with identifying false misbehavior reports.

[5] It has two phases in query processing; in first phase query issuing node collects information of scores from each node. Based on these received information query issuing node calculates threshold values. In second phase query issuing node transmits a query attached with the threshold value. Nodes reply with items which have scores greater than or equal to threshold.

[6] sensor network generate a large amount of data during monitoring phase, so energy conservation is essential in network. This is a history based approach which estimates thresholds by prune-query algorithms. Here query messages directed to right directions by cached data.

## 3. METHODOLOGY

The method includes mainly five phases: 1) Top-k query processing. 2) Attack detection. 3) Malicious node identification. 4) Grouping of nodes 5) Location identification.
The proposed methodology contains a top-k query processing phase. Each node holds a table having the victims and its corresponding score, the query result is taking from this tables. This paper focus on avoiding the attack called DRA. Query issuing node identifies this attack from the list of results it retrieves from different paths. It compares the results and narrows down the candidates. The malicious node is taken out from the candidate list and calculating the final result by avoiding the result given from that path. The attack detection algorithm and candidate generation algorithm is discussed later in this paper.

### 3.1 Over view

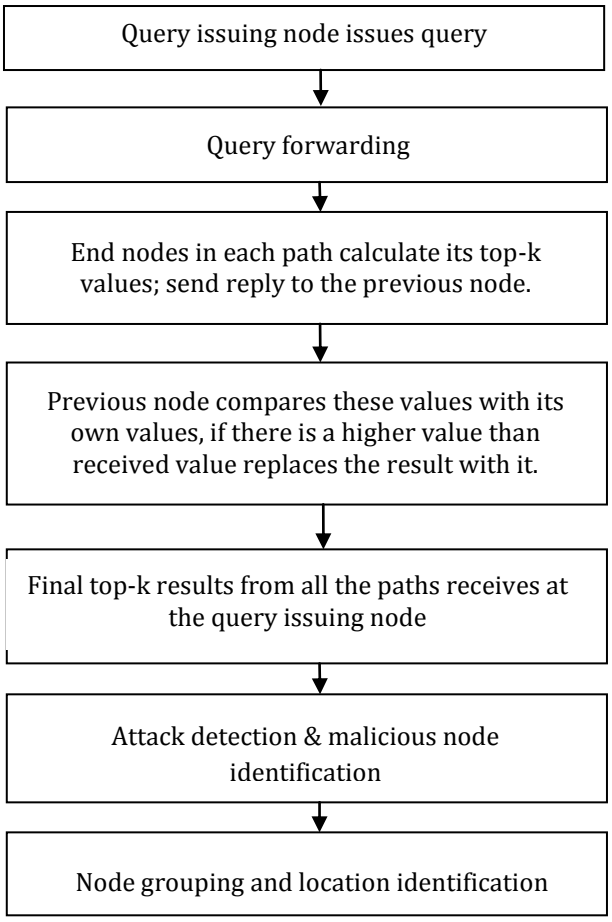


**Fig -2**: Overall system flow

### 3.2 Top-k query processing

The query issuing node floods the query with the query condition having the value of k. If the query issuing node wants the data having three highest scores it set the value of k =3 and floods in the network to through every paths. The query also includes identifier of issuing node and the path through which the query is forwarding. The query issuing node set a Reply Time (RT).Upon receiving the query at the end of each path, the end node calculates its data having k highest scores and send reply to its previous node, after merging its values, and the values sent by the end node it calculates the top k values and send to its previous node. This repeats until the reply reach at the query issuing node. The reply keeps track of the reply path in a path-list. The path-list includes IDs of reply path and top values of each node. So, the query issuing node gets two lists from every paths as reply. The first list includes list of top k data items that is the query result required by the query issuing node. And the second list is a list of paths where the reply has been

forwarded along with its top value. The reply is generating when RT has passed.

### 3.3 Attack Detection

After the query issuing node gets replies from every path, it is going to detect the Data Replacement Attack. To detect the DRA it takes the data from top-k list and path-list, and compares its score values. The query issuing node detects an attack if the score of path file greater than any score of top-k list. The path having that ID set as malicious path.

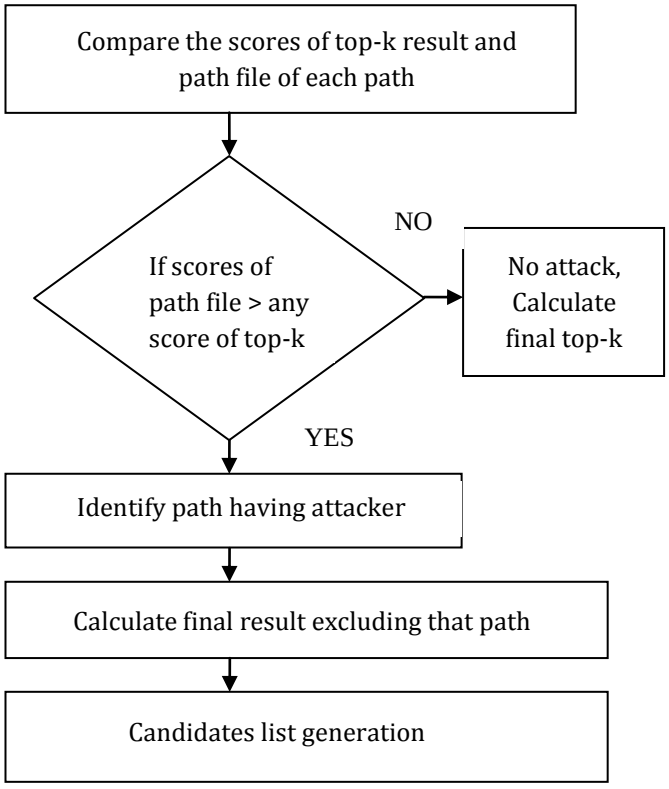


**Fig -3**: Attack Detection

### 3.4 Malicious Node Identification

After detecting the attack the query issuing node wants to identify the attacker node.

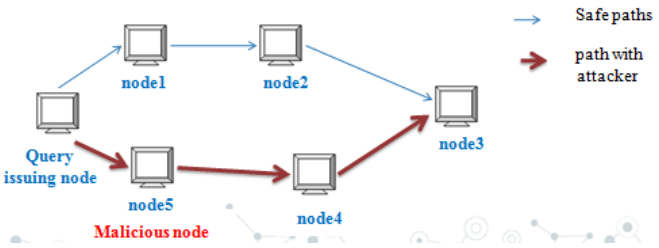


**Fig -4**: Candidate-list Generation

For malicious node identification query issuing node generates a candidate list which includes IDs of the nodes in malicious path. Then the malicious node is taken out from the list by applying the following malicious node detection algorithm.Figure-4 shows the attacking path in red line, after identifying this path as malicious the query issuing node insert node 5 and node 4 to candidate-list.

Malicious node detection algorithm is given below,

Algorithm1: Malicious node detection

**For each** nodes in path file excluding the malicious path
Insert ID of the nodes to safe-id file
**For each** node ID in candidates do
**If** (No. of Candidates == 1) then
**Return** Candidate as a Malicious Node
**Else if** (No. of Candidates > 1) then
**For each** node ID do
Compare ID with id values of safe-id file if a match found then,
Remove the candidate from candidate-list
**End if**
**End for**
**End for**
**The remaining node will be the attacker**

If there is only one node in the candidate list then it will be the attacker. If there is multiple nodes in the candidate list then safe paths are taken by avoiding the malicious path, then the id of each node on the path are taken. It is going to be compared with the ids of the candidates. If the candidates who have the possibility of being attacker is taken if it matches with any id of the safe paths then it is removed from the candidate list. Do this repeatedly .the remaining node or nodes will be the malicious node. This can be identified and labeled.

### 3.5 Grouping of Nodes

The grouping of nodes is done for the rescue operations. In the case of a real time application such as disasters there will be nodes which collects the information from the people who are mostly affected by the disaster, and the nodes who are least affected. The grouping is done based on these criteria. The nodes are grouped by the score values of each data item it have. Each node has a data set which is ordered by a score which shows the priority of each data. The nodes are grouped using this score value. If the data score value is high then it is added to a group called Red alert. If data score value has second group of priority then it is grouped to Orange alert group. If the data scores of the data have less priority then it is grouped to Yellow alert. Here taking data score above 90 as red alert. Group the nodes having scores between 70 and 90 to orange alert. Nodes having data score below 70 to yellow alert. The malicious node is not avoided

it is grouped into yellow alert by considering the possibility that it may be a selfish node not an attacker.

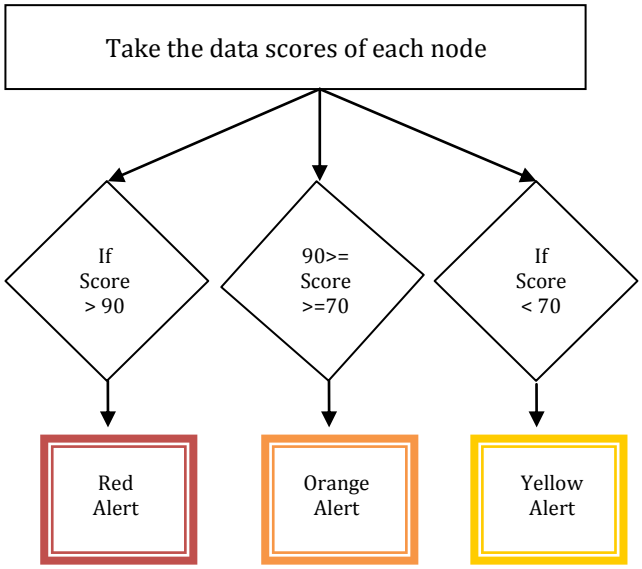


**Fig -5**: Grouping of nodes

### 3.6 Location identification

After grouping of nodes to Red alert, Orange alert, Yellow alert the rescue operator wants to immediately identify the nodes having Red alert. For providing the rescue services without any delay the rescue operator wants to properly identify the exact location of the peoples who needs emergency services. Location identification is done for these fast and efficient rescue operations. Positions of nodes are identified by taking the vector spaces from the mobility model.

## 4. CONCLUSIONS

This paper proposed a Top-k query processing and malicious node identification method for MANETs. The Top-k query processing method gives an efficient Top-k query results for the query issuing node. The query retrieval methods can be used for the disaster rescue purposes. Each node stores the data of the peoples in its location who need rescue; this is collected by rescue operators for the rescue operations. An attack called data replacement attack which replaces the high score data with its low score data items is possible. It will affect the efficiency in rescue operations, In order to avoid DRA the paper proposes an attack detection method by query issuing node and also do the malicious node identification. After identifying the malicious node the nodes are grouped to three groups Red alert, orange alert, yellow alert based on their scores of data items. Finally the locations of peoples in different groups can be identified by the positions of nodes for the rescue operations.

## REFERENCES

[1] Takuji Tsuda,Yuka Komai,Takahiro Hara And Shojiro Nishio “Top-k query processing and malicious node identification based on node grouping in in MANETs”, IEEE Access 2016.

[2] 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.

[3] D.Amagata.Y. Sasaki, T.Hara, and S.Nishio, “A robust routing method for top-k queries processing in mobile adhoc networks”, in Proc. MDM, Jun. 2013.

[4] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami “EAACK—A Secure Intrusion-Detection System for MANETs " ,IEEE transaction. 2013.

[5] Y.Sasaki, T. Hara, and S. Nishio, "Two-phase top-k query processing in mobile ad hoc networks " ,in Proc. NBiS,Sep. 2011.

[6] Qunhua Pan, Shuwang ,Minglu,Min-You Wu “Energy Efficient Top-k Query Processing in Dynamic Sensor Network.”,IEEE 2010.