Top-K Query Processing in MANETS on Malicious Node Identification

D. Porselvi[1] B. Gopinathan[2]
[1,2]Adhiyamaan College of Engineering

Abstract— 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 paper, 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. It is suitable for a hub to share information about the distinguished harmful hubs with different hubs. . We lead proliferation tests by using a framework test framework, QualNet5.2, to watch that our procedure finishes high exactness of the question result and recognizes malicious hubs.

Key words: Ad Hoc Networks, Top-K Query Processing, Data Replacement Attack, Grouping

I. INTRODUCTION

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). Then again, in MANETs, if a typical node gets to be pernicious attributable to an assault from outside the system, the pernicious node tries to upset the operations of the framework. In this paper, we characterize another sort of assault called information substitution assault (DRA), in which a vindictive hub replaces the got information things (which we call the neighborhood beat k result) with superfluous yet appropriate information things (e.g., its own low-score information things). Since DRAs are a solid attack, and more hard to recognize than other conventional sorts of attack, some particular component for guarding against DRAs are required.

A. Existing System

The query-issuing node which issues a query firstly in the network sends a message for constructing routing table, and then nodes that receive the message reply the information on scores of data items held by them. The receiver stores the information in the received ranking table into own routing table. The receiver sets query addresses for all ranks in own routing table as the identifier of the node that sent the ranking table to it. The receiver updates query addresses for ranks to its own identifier if it holds the corresponding data items.

II. RELATED WORK

In this segment, we survey existing studies on secure directing, top-k inquiry handling strategies, and notoriety frameworks.

A. Secure Routing Methods

In the field of MANET, secure directing conventions ensure against falsification of information and DoS attacks have been all around concentrated on. Secure directing conventions generally utilize information transmission along various courses (from the source hub to the destination hub) [6], [8], [9], and information encryption utilizing symmetric or open keys [6], [9], [7]. In [6], the creators have proposed a strategy in which the source hub decides numerous sheltered courses (from the source hub to the destination hub) by encoding the course ask message utilizing a hash capacity before sending information things.

B. Top-k Query Processing Methods

In the field of database frameworks and conveyed frameworks, top-k inquiry is viable to recover just the required information things in a extensive measure of information things. In [2], [5], [10], the creators have proposed strategies to decrease vitality consumption and traffic in unstructured P2P systems or remote sensor systems, by empowering hubs to lter pointless information things. In any case, these techniques don't ensure against DRA, also, are unsatisfactory for use in MANETs, since they are definitely not adjusted to hub portability.

III. MODULES

A. Network Design, Top-K query Processing, Data Replacement attack

1) Network Design

The framework environment is thought to be a MANET built by portable hubs held by individuals from a very critical community oriented work, for example, save operations and military undertakings in which the individuals issue beat k inquiries to productively gain information things. For a situation of save operations, emergency vehicle clews need to get casualties in a basic condition. The assailants, for example, dread hack a hub which a rescue vehicle clew holds in light of the fact that the aggressors plan to spread the harm for quite a while. The scores of information things can be figured in light of the question condition and indicated scoring capacities.

2) Top-K Query Processing

a) Query Forwarding

To start with, the inquiry issuing hub surges a question over the whole system. The inquiry comprises of the hub identifier of the question issuing hub (Query-issuing

nodeID), the question identifier of the inquiry (Query ID), the quantity of asked for information things (k), the question condition, and a rundown of the hub identifiers of hubs on the way along which the question message is to be transmitted (Query way). In particular, the question issuing hub, Mp, indicates the inquiry condition and the quantity of asked for information things, k. At that point, Mp transmits a question message whose Query way incorporates its identifier, Mp, to its neighbor hubs. A hub, Mq, which gets the inquiry, transmits it as indicated by sending a Query Algorithm.

b) Reply Forwarding

At the point when Query has passed, every hub sends back an answer message, which incorporates its own particular hub identifier (Sender hub ID), the identifier of the following hub along the answer course (Dest node ID), a rundown of the information things (counting their scores) and the hub identifiers of the hubs having them (Data list), and a rundown outlining the answer message courses, i.e., a rundown of the sets of sender and next hub identifiers (Forwarding Route).

3) Detecting Attacks

a) Data Replacement Attack

Each node calculates the local reputation scores of other nodes from correctness of received files, and foods the score information in the network. Then, each node calculates the global reputation score from its own and received local scores. At last, it determines the node whose global score is lower than a threshold as the malicious nodes. In have proposed methods in which each node manages the reputation values of its neighboring nodes in MANET.

B. Malicious Node Identification

After the node grouping every hub indisputably decides malevolent hubs in light of the data about noxious hubs recognized by hubs in each gathering. Here, there are three types of groups, i.e., a group made out of (i) just typical hubs, (ii) just noxious hubs, and (iii) both ordinary and malevolent nodes. The hubs distinguished as malicious by all nodes in a group of (i) or (iii) are surely malicious nodes. Only in a group of (iii), normal nodes can be identified as malicious by all nodes which collaboratively attack on FNA.

C. Algorithm

1) Identification of A Malicious Node

1) INPUT: Candidate
2) OUTPUT: MaliciousNode
3) /* Mp starts to inquire */
4) for every i in Candidate.size do
5) if InqRoute incorporate different competitors in Candidate at that point
6) /* End system without inquisitive */
7) break
8) else if jump check to Candidate > 1 then
9) /* Send an ask message */
10) Send MNI-INQ to Mdesti to ask information things that Candidate[i] sent
11) end if
12) /* Mv gets an ask message */
13) if Mv gets MNI-INQ then
14) Send MNI-INQ to the following hub of Mv in InqRoute
15) end if
16) /* A noxious hub hopeful gets an ask message */
17) if Mdesti gets MNI-INQ then
18) Send MNI-IREP including scores of information things sent by Candidate[i] to Mp
19) end if
20) /* Mu gets an answer message for the request */
21) if Mu gets MNI-IREP then
22) Send MNI-IREP to sender MNI-INQ
23) end if
24) /* Mp gets an answer message for the request */
25) if Mp gets MNI-IREP then
26) /* the inquiry issuing hub identifies the noxious hub */
27) if scores incorporates the score of the missing information things in worldwide Top-k result then
28) return Candidate[i-1]
29) end if
30) end if
31) end for

2) Graph for Data Accessibility

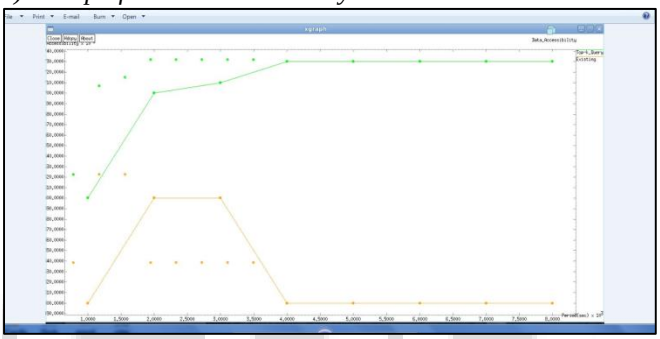

Fig. 1: Graph for Data Accessibility:

IV. CONCLUSION

In this paper, we have proposed strategies for top-k inquiry handling and pernicious hub identication in light of hub gathering in MANETs. With a specific end goal to keep up high exactness of the inquiry result and identify attacks, hubs answer with k information things with the most astounding score along various courses. In the wake of distinguishing assaults, the question issuing hub contracts down the pernicious hub applicants and after that tries to distinguish the pernicious hubs through message trades with other hubs. At the point when numerous vindictive hubs are available, the inquiry issuing hub will be unable to recognize every noxious hub at a solitary question

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. 251_256.
[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. 174_185.
[3] 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. 329_338.
[4] H. Chan, A. Perrig, and D. Song,"Secure hierarchical in network aggregation in sensor networks,"in Proc. CCS, 2006, pp. 278_287.
[5] 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. 266_270.
[6] 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. 12_23.
[7] Y.-C. Hu, D. B. Johnson, and A. Perrig, ``SEAD: Secure ef_cient distance vector routing for mobile wireless ad hoc networks," Ad Hoc Netw., vol. 1, no. 1, pp. 175_192, Jul. 2003.
[8] 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. 338_346, 2007.
[9] S. J. Lee and M. Gerla, ``Split multipath routing with maximally disjoint paths in ad hoc networks," in Proc. ICC, vol. 10. Jun. 2001, pp. 3201_3205.
[10] X. Liu, J. Xu, and W. C. Lee, ``A cross pruning framework for top-kdata collection in wireless sensor networks," in Proc. MDM, May 2010, pp. 157_166.

