ISSN (online): 2349-6010

A Survey on Top-K Query Processing and Malicious Node Identification in MANETS

D. Porselvi
Department of Computer Science and Engineering
Adhiyamaan College of Engineering

B. Gopinathan
Department of Computer Science and Engineering
Adhiyamaan College of Engineering

Abstract

In versatile imprompt systems (MANETs), it is powerful to recover information things utilizing top-k query. Notwithstanding, precise results may not be obtained in situations when vindictive nodes are available. It is expected that pernicious nodes endeavor to supplant vital information things with pointless ones (we call these as data replacement attacks attacks), and propose techniques for top-k inquiry preparing and malicious node identification taking into account node gathering in MANETs. Keeping in mind the end goal and to keep up the exactness of the query result, answer with nodes k information things with the most noteworthy score along different courses, and the query issuing node tries to identify attacks from the data appended to the answer/reply messages. In the wake of distinguishing attacks, the query issuing node tries to recognize the malevolent nodes through message trades with different nodes. At the point when different malicious nodes are available, the inquiry issuing node will most likely be unable to recognize every single malicious node at a solitary inquiry. It is viable for a node to share data about the identified malicious nodes with other nodes. In our strategy, every node separates all nodes into gatherings by utilizing the likeness of the data about the identified malignant nodes. At that point, it identifies noxious nodes in view of the data on the gatherings. By using network simulator and OTCL, we verify, through simulation experiments, that the proposed top-k query processing method achieves high accuracy of the query result, and that the malicious node identification method effectively identifies a malicious node.

Keywords: HyperCup Topology, Confidant, Spread, Routing table, Ariadne, Sead

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. For this situation, the client whose system contains the pernicious..node will regularly keep on operating the framework ordinarily, unconscious of the risk, while the noxious node may execute an assortment of attacks (e.g. Denial of Service (DoS) assault for example, blackhole attack).

A chance to consider a reason for pernicious node attacking top-k inquiry handling. Fundamentally, noxious nodes endeavor to disturb inquiry issuing node's obtaining of the worldwide top-k result for a long stretch, without being distinguished. In any case, DoS attacks in MANETs have been effectively concentrated on for long years, and subsequently, utilizing existing methods, such attacks can be uncovered by the question issuing node then again middle nodes. Here, a wonderful normal for top-k question handling is that the inquiry issuing node does not know the worldwide top-k come about heretofore.

II. DATA REPLACEMENT ATTACK

Hence, regardless of the possibility that a vindictive node replaces high-score information things with its own low-score ones, while transferring the information things, it is difficult for the question issuing to distinguish the assault, and it might trust that all the received data items with k highest scores are the global top-k result. In this paper, we define a new type of attack called data replacement attack (DRA), in which a malicious node replaces the received data items (which we call the local top-k result) with unnecessary yet proper data items (e.g., its own low-score data items). Since DRAs are a strong attack, and more difficult to detect than other traditional types of attack, some specific mechanism for defending against DRAs are required.

Top-k inquiry preparing and Malicious node identification strategies again DRAs in MANETs. In top-k inquiry preparing strategy, with a specific end goal to keep up exactness of inquiry result and distinguish attacks, nodes answer with information things with k most astounding scores along various courses. Also, to empower recognition of DRA, answer messages incorporate data on the course along which answer messages are sent, and along these lines the inquiry issuing node can know the information things that legitimately have a place with the message. In the malicious node identification technique, the inquiry issuing node contracts down the malignant node applicants, utilizing information in the got message, and after that solicitations data on the information things sent by these hopefuls. Along these lines, the question issuing node can recognize the malignant node.

III. RECOGNITION OF MORE THAN ONE MALICIOUS NODES

At the point when there are numerous pernicious nodes in the system, it is difficult to distinguish all the pernicious nodes in a single query. By utilizing our techniques, nodes are prone to distinguish the noxious nodes which are close to their own area, while they scarcely distinguish the malignant nodes which are a long way from their own area. Thusly, with a specific end goal to rapidly recognize more vindictive nodes, it is compelling to share the data about the identified vindictive nodes with different nodes. In this case, nonetheless, a pernicious node may proclaim fake information that cases ordinary nodes as the pernicious nodes (false notification assault (FNA)).We require some technique to effectively recognize the malignant nodes against FNAs.

IV. FALSE NOTIFICATION ATTACK

In this manner, in our vindictive node identification strategy, after nodes share the malignant node identification information, every node isolates all nodes into a few gatherings in view of the closeness of the data. At that point, the node decides the judgment of malevolent nodes in light of the judgment after effect of every gathering. In our strategy, regardless of the fact that malignant nodes claim that typical nodes are the malignant nodes, there is a unequivocal contrast in the way of the data had by typical and malignant nodes concerning the identified malevolent nodes, and in this manner, the ordinary nodes can without much of a stretch recognize the malignant nodes. Besides, regardless of the possibility those noxious nodes blend the right data on malevolent nodes idenfied by other typical nodes with their fake data, so as to expand their similitude with typical nodes, the typical nodes in the same gathering will in any case surely recognize the malignant nodes, however not typical nodes. Along these lines, the data from the malevolent nodes can be expelled and there is little influence of FNAs.

V. MAINTAINING DATA TRAFFIC

They introduced the benefits of best match/top-k queries in the context of distributed peer-to-peer information infrastructures and showed how to extend the limited query processing in current peer-to-peer networks by allowing the distributed processing of top-k queries, while maintaining a minimum of data traffic [1].

Relying on a super-peer backbone organized in the HyperCuP topology shows how to use local indexes for optimizing the necessary query routing and how to process intermediate results in inner network nodes at the earliest possible point in time cutting down the necessary data traffic within the network.

The algorithm is based on dynamically collected query statistics only, no continuous index update processes are necessary, allowing it to scale easily to large numbers of peers, as well as dynamic additions/deletions of peers. This approach is to always deliver correct result sets and to be optimal in terms of necessary object accesses and data traffic [1].

VI. NEED FOR CONFIDANT

A protocol, called CONFIDANT, for making misbehavior unattractive; it is based on selective altruism and utilitarianism. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation.

Trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes. We present a performance analysis of DSR fortified by CONFIDANT and compare it to regular defenseless DSR. It shows that a network with CONFIDANT and up to 60% of misbehaving nodes behaves almost as well as a benign network, in sharp contrast to a defenseless network[2].

VII. NETWORK LIFE TIME

It mainly focus on evaluating top-k queries in an energy-efficient manner such that the network lifetime is maximized. To achieve that, we devise a scalable, filter-based localized evaluation algorithm for top-k query evaluation, which is able to filter out as many unlikely top-k results as possible within the network from transmission[3].

Among various queries, top-k query is one of the fundamental operators in many applications of wireless sensor networks for phenomenon monitoring.

VIII. ROUTING TABLE

They followed a method called routing method for Top-k query processing in MANETS. In this method mobile nodes sends a top-k query, which will refer to the routing table that consists of rank of scores of data items in which queries are forwarded to obtain the necessary data items, which reduces the traffic and high accuracy of the query result is obtained[4].

IX. SPREAD

It introduced a scheme called security protocol for reliable Data delivery (SPREAD) to enhance the data safety in MANET since security is a critical issue in MANETs. The proposed SPREAD scheme aims to provide further protection to secret messages from being hacked when -they are delivered across the insecure network. Maximum node disjoint Paths algorithm and multipath routing techniques are used as methodology [5].

A. Protocols:

The Denial of service attacks in sensor networks will make real-world damage to health and safety of people. Sensor networks help facilitating large scale real time data processing in complex environments using sensor network protocols and RAP protocols. Design time considerations of security offers the most effective defense against attacks on availability[6].

B. Techniques:

It is said that Ad hoc network do not rely on a physical infrastructure or a central administration entity. To control the user across access in ad hoc networks a self-organised mechanism is used. This paper proposes mechanism to authenticate and monitors nodes with so called controller sets using a techinique called cryptography [7].

X. ARIADNE

Prior research in ad hoc networking has generally studied the routing problem in a non-adversarial setting, assuming a trusted environment. In this paper, we present attacks against routing in ad hoc networks, and we present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of-Service attacks. In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives[8].

A. SEAD Protocol:

The Secure and Efficient Ad hoc Distance vector routing protocol (SEAD) is based upon the DSDV routing protocol. It uses efficient one-way hash functions to authenticate the lower bound of the distance metric and the sequence number in the routing table.

The advantage of using SEAD protocol is that it is robust against multiple uncoordinated attackers, active attackers or compromised nodes. It uses efficient, inexpensive cryptographic primitives and this plays an important role in the computation and bandwidth-constrained nodes. The disadvantages of SEAD are that it doesn't provide a way to prevent an attacker from tampering with "next hop" or "destination" columns. Instead, it relies on doing neighbor authentication, which is a bad thing. Hash chains are consumed very fast. [9]

The threat of topology-exposure and proposes a Topology-Hiding Multipath Routing protocol (THMR). THMR doesn't allow packets to carry routing information, so malicious nodes cannot deduce topology information and launch various attacks based on that. The protocol can also establish multiple node-disjoint routes in a route discovery attempt and exclude unreliable routes before transmitting packets. THMR does not contain link connectivity information in route messages. Thus no node can deduce network topology by capturing route messages and the topology is hidden. THMR can also find as many node disjoint routes as possible, defend against attacks and exclude unreliable routes [10].

XI. CONCLUSION

Malicious node identification using Top-k Query in MANETs will help in detecting attacks and in maintaining high accuracy. Traffic can also be minimized and by using energy efficient Life time can be increased, since energy is highly prioritized in MANETS. The protocols used can help in avoiding the pernicious nodes. So that data loss is avoided and information is transferred at higher rate.

REFERENCES

[1] 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.
[2] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol,"in Proc. MobiHoc, 2002, pp. 226_236.
[3] B. Chen, W. Liang, R. Zhou, and J. X. Yu, "Energy-efficient top-k query processing in wireless sensor network," in Proc. CIKM, 2010,pp. 329_338.
[4] 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.
[5] W. Lou, W. Liu, and Y. Fang, "SPREAD: Enhancing data con_dentiality in mobile ad hoc Networks," in Proc. INFOCOM, vol. 4. Mar. 2004,pp. 2404_2413.
[6] A.D. Wood and J. A. Stankovic, "Denial of service in sensor networks,"Computer, vol. 35, no. 10, pp. 54_62, Oct. 2002.
[7] 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.

[8] 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.
[9] 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. 175_192, Jul. 2003.
[10] Y. Zhang, G. Wang, Q. Hu, Z. Li, and J. Tian, "Design and performance study of a topology-hiding multipath routing protocol for mobile ad hoc networks,"in Proc. INFOCOM, Mar. 2012, pp. 10_18.