Malicious Node Identification Based On Top-K Query Processing In MANETS

Haritha.K[1], G.Chithra Ganapathy[2], Dr.N Sudha[3]
[1, 2] Dept of Computer Science&Engineering
[2] Associate Professor Dept of Computer Science&Engineering
[3]Professor Dept of Computer Science&Engineering
[1, 2, 3] CMS College of Engineering And Technology , Coimbatore,Tamil Nadu

Abstract- *In mobile ad hoc networks (MANETs), it is effective for mobile nodes to retrieve data items using top-k queries, in which data items are ordered according to a particular attribute score, and the query-issuing node acquires the data items with the k highest scores. However, accurate results may not be acquired in environments where malicious nodes are present. In top-k queries, it is important to neutralize the Data Replacement Attack (DRA). The DRA is defined as the malicious nodes attempt to replace necessary data items with unnecessary ones. The proposed method addresses top-k query processing and malicious node identification against data replacement attack in MANETs. In the top-k query processing method, in order to maintain accuracy of the query result, nodes reply with data items with the k highest scores, along multiple routes. Moreover, to enable detection of data replacement attacks, reply messages include information on the route along which reply messages are forwarded, and thus the query-issuing node can know the data items that properly belong to the message. In the malicious node identification method, the query-issuing node first narrows down the malicious node candidates, using the received message information, and then requests information on the data items sent by these candidates. In this way, the query-issuing node can identify the malicious node. When multiple malicious nodes are present, the query-issuing node may not be able to identify all malicious nodes at a single query. It is effective for a node to share information about the identified malicious nodes with other nodes. In the proposed method, each node divides all nodes into groups by using the similarity of the information about the identified malicious nodes. Then, it identifies malicious nodes based on the information on the groups. In this case, however, a malicious node may declare fake information that claims normal nodes as the malicious nodes. This type of attack is called as false notification attack (FNA) and the node who is performing FNA only called as Liar Nodes (LN). Identification of the LN is also based on the information on the groups itself. By using Optimized Link State Routing Protocol (OLSR) we are designing a message authentication method to prevent malicious nodes from performing FNA.*

Keywords- Mobile Ad-Hoc Networks, Anycast routing, Energy Efficiency.Channel Congestion.

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each mobile device can be called as a node which has communication capabilities. Nodes can communicate directly or indirectly with each other. The mobile devices can communicate each other directly if they fall in the radio coverage range of each other otherwise the node can use the concept of multihop. Each node behaves like Station and Router. All the nodes participate in the routing and the performance may depend upon the cooperation between nodes. MANETs are useful where there is no infrastructure is or installation is not possible. The characteristics of MANETs are operating without any central coordinator/base station, dynamic topology, energy-constrained operation, longer transmission range due to multi-hop relay, self-configuring, constraint bandwidth, distributed operation. Rapid deployable, Self-Configurable, Mobility, Does not require any infrastructure to work, Cost effective, less time consuming, more robust than cellular system are the main advantages of MANETs. Dynamic changing topology, Limited bandwidth, Limited battery power, Security issues are the very few disadvantages of MANETs.

Due to the poor resources (i.e., the communication bandwidth and the battery life of mobile nodes are limited) for each nodes in the MANET, it is effective to retrieve only the necessary data items using top-k query. The query issuing node first floods a query over the entire network, and then, each receiving node replies with data items with the k highest scores. The query-issuing node acquires the data items with k highest scores in the network (the global top-k result).

On the other hand, in MANETs, if a normal node becomes malicious owing to an attack from outside the network, the malicious node tries to disrupt the operations of the system. In this case, the user whose network contains the

malicious node will typically continue to operate the system normally, unaware of the threat, while the malicious node may execute a variety of attacks (e.g. Denial of Service (DoS) attack such as black hole attack).A malicious node is defined as node seeking to deny service to other nodes in the network. The node which modifies data before, during or after transmission is also known as malicious node. Due to the presence of malicious nodes in the MANET, source and destination nodes became unable to communicate with each other in the network.

Consider a purpose of malicious node attacking top-k query processing. Basically, malicious nodes attempt to disrupt query-issuing node's acquisition of the global top-k result for a long period, without being detected. Here, a remarkable characteristic of top-k query processing is that the query-issuing node does not know the global top-k result beforehand. Therefore, even if a malicious node replaces high-score data items with its own low-score ones, when relaying the data items, it is difficult for the query-issuing to detect the attack, and it may believe that all the received data items with *k* highest scores are the global top-k result. The attacks in the MANETs due to the malicious nodes are basically classified into two types. They are: (1). Data Replacement Attack (DRA) and (2). False Notification Attack (FNA). DRA is a new type of attack in which a malicious node replaces the received data items known as the local top-k result with unnecessary data items for example its own low-score data items. Since DRAs are a strong attack, and more difficult to detect than other traditional types of attacks, some specific mechanism for defending against DRAs are required. A malicious node may declare fake information that claims normal nodes as the malicious nodes is called as the FNA. The one who is doing only the attack called FNA is known as the liar nodes where it is represented as LN.

The main objective of the project is that addressing the issue of identification of liar nodes (*LN*s), and designing a message authentication method using the OLSR to prevent malicious nodes from performing FNA in MANETs.

MANET is currently using in many real time applications like disaster management, whether reporting etc. Top k query processing is the popular way to get data from MANET. It is important to keep the top k query results error free. .

II. RELATED WORK

Top-K Query Processing Method [1] Exact top-k query processing has gained more and more attention recently because of its wide use in many fields, such as information retrieval, multimedia databases , P2P and sensor networks etc.The main reason for such attention is that top-k queries avoid overwhelming the user with a large number of uninteresting answers that are resource-consuming. However, two main reasons convince us to abandon exact top-k query processing. First, the top-k query concept is heuristic anyway. Hardly any user is interested in all the exact k answers of a top-k query. Instead, they may be only interested in one or several relevant objects in the top-k answers. So, due to the subjective judgment of the user, missing the truly best answers is inherent and unavoidable. This argument enlightens us to relax exact top-k query to approximate top-k query. Second, the cost of processing exact top-k queries is highly expensive for datasets with huge volume, and the size of datasets in practice is always quite huge. So it's intriguing to answer approximate top-k query instead of exact top-k query. Even though the methods used in information retrieval, multimedia databases, P2P and sensor networks etc. helps to reduce energy consumption and traffic by enabling nodes to filter unnecessary data items but also these methods are unsuitable for use in MANETs and do not protect against DRA, because they are not adapted to node mobility. In proposed top-k query processing methods for MANETs, adapted to the node mobility. With these methods, the query-issuing node floods the query message attached with some score information. Each node then estimates the k-th score of the data item and sends back data items whose scores are equal to or greater than the estimated one. This method can, therefore, decrease the number of transmitted data items. However, there is still a drawback that queries are forwarded to all nodes in the network by flooding. Thus, many nodes that do not contribute to the data items with k- highest scores have to send redundant top-k queries and replies. As a result, there is a high level of traffic.

In most current reputation systems a node collects locally-generated node feedbacks and aggregates them to yield the global reputation values for others based on periodical information exchanges between neighbours. The node whose reputation is below a predefined threshold is considered as selfish and put into a blacklist, otherwise as trustworthy or malicious. However, the systems suffer from a number of problems. First, they lack efficient mechanisms to collect and propagate reputation information. Periodical information exchanges, keeping redundant reputations in each node, and broadcasting to query reputations consume significant resources, failing to achieve high scalability. Second, reputation Calculation based on partial local information, which may include false information, may result in insufficiently accurate reputation evaluation to truly reflect node behaviours. Third, solely relying on reputation system is not effective enough to thwart uncooperative behaviours.

Secure Routing Methods Secure routing protocols commonly employ data transmission along multiple routes (from the source node to the destination node) and data encryption using symmetric or public keys.

The design and performance evaluation of a new on-demand secure ad hoc network routing protocol, called Ariadne that withstands node compromise and relies only on highly efficient symmetric cryptography. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents a large number of types of Denial-of-Service attacks. Ariadne is more secure, more efficient, or more general. Ariadne can authenticate routing messages using one of three schemes: shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signatures.

A novel scheme, called Secure Protocol for REliabledAta Delivery (SPREAD) [18], to statistically enhance data confidentiality in a MANET. The fundamental idea of SPREAD is shown in figure 2.3. Assume that the secret message is sending through a single path; the enemy can compromise it by compromising any one of the nodes along the path. However, if the secret message is dividing into multiple pieces, and sending these multiple pieces via multiple independent paths, then the enemy has to compromise all the pieces from all the paths to compromise the message. Improved security can be expected by this means. Here, to compromise the message, the enemy must accomplish at least two things. First, the enemy must physically intercept all pieces of the message. This can be done by either eavesdropping or compromising nodes. Either way, by spreading the message pieces over multiple paths, the enemy will have more difficulty to collect all the pieces. Secondly, link encryption between neighbouring nodes and each link with different keys. Although, in general, key management is problematic in a MANET, the establishment of a shared session key between neighbouring nodes is not that difficult. Link encryption is also widely used to prevent the traffic analysis. So even the enemy collected all the pieces, he/she has to decrypt all of them. The decryption can be done by either compromising the nodes or by brute-force type of attacks or traffic analysis, while the latter requires a large amount of encrypted data by the same key. The more data, the better chance the decryption. By spreading the traffic onto multiple paths, it is harder for the enemy to decrypt the message. However, these methods neither assume top-k queries nor protect against DRA, and thus cannot be directly applied to the problem.

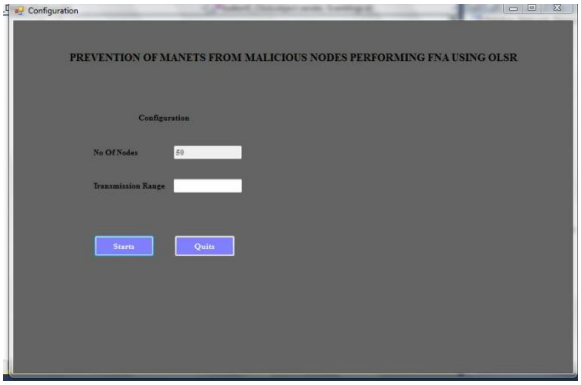
A novel scheme, called Secure Protocol for REliabledAta Delivery (SPREAD) [18], to statistically enhance data confidentiality in a MANET. The fundamental idea of SPREAD is shown in figure 2.3. Assume that the secret message is sending through a single path; the enemy can compromise it by compromising any one of the nodes along the path. However, if the secret message is dividing into multiple pieces, and sending these multiple pieces via multiple independent paths, then the enemy has to compromise all the pieces from all the paths to compromise the message. Improved security can be expected by this means. Here, to compromise the message, the enemy must accomplish at least two things. First, the enemy must physically intercept all pieces of the message. This can be done by either eavesdropping or compromising nodes. Either way, by spreading the message pieces over multiple paths, the enemy will have more difficulty to collect all the pieces. Secondly, link encryption between neighbouring nodes and each link with different keys. Although, in general, key management is problematic in a MANET, the establishment of a shared session key between neighbouring nodes is not that difficult. Link encryption is also widely used to prevent the traffic analysis. Secure Routing Methods [3]Secure routing protocols commonly employ data transmission along multiple routes (from the source node to the destination node) and data encryption using symmetric or public keys. The design and performance evaluation of a new on-demand secure ad hoc network routing protocolIn this method the existence of only one malicious node in the entire network can only be identified. However, in real environments there may be multiple numbers of malicious nodes present in the entire network. In this case, since nodes must increase the number of routes along which reply messages are sent, high traffic volume is required to remain high accuracy of the query result. After the query-issuing node has received all the reply messages, it confirms the received signature lists, and thereby detects any DRAs and identifiers the respective malicious nodes. If the query-issuing node identifies malicious nodes, it shares this information by flooding a notification message over the entire network, including the identifiers of the malicious nodes, and the signature lists in which these nodes have replaced data items with their own lower-score items. Nodes receiving this notification message for the first time decrypt the signature lists attached to the received message, and confirm that the nodes identified as malicious have actually performed DRAs. The traffic required for top-k query processing is large, resulting low accuracy of the query result especially when *k* is large.

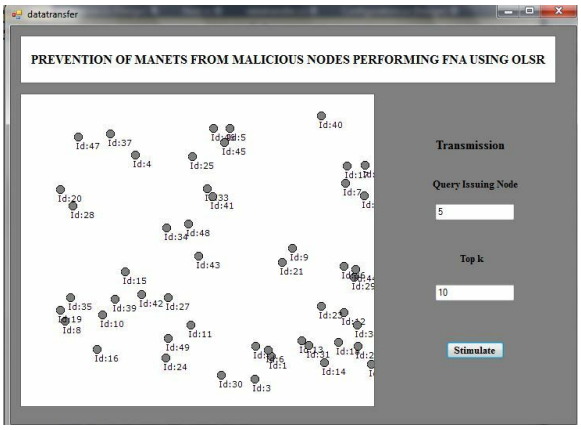
III. PROPOSED METHOD

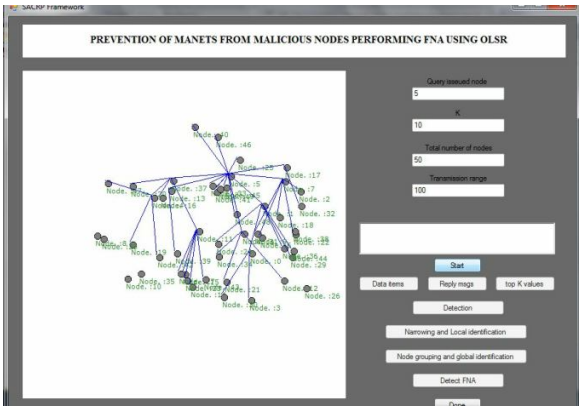
The proposed top-k query processing method addressing the issue of identification of liar nodes (*LN*s), and also to designing a message authentication method to prevent malicious nodes from performing FNAs. For the message authentication method, the proposed system adopts the idea of the OLSR routing protocol. OLSR is table-driven and pro-active and utilizes an optimization called Multipoint Relaying (MPR) for control traffic flooding. A node's one hop neighbour which has been chosen to forward packets is called as MPR. The secure routing functions for OLSR routing protocol are: (i) Authentication of nodes (ii) Authentication of control message (iii) Key updating (iv)Periodical re-authentication (v) Authentication at node's movement (vi) Ad hoc sharing. Here the proposed method is adopting the feature authentication of nodes.

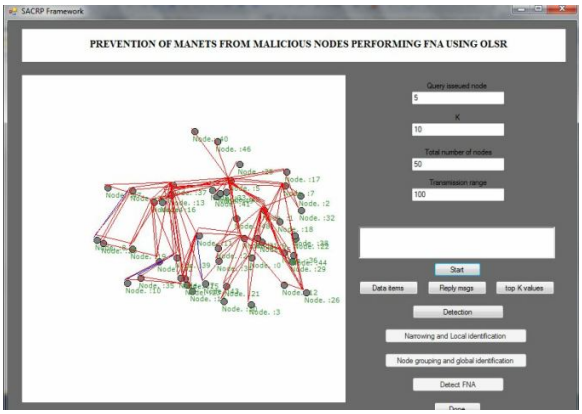
In the proposed system the query issuing node first generates an authentication message and pass this to all the nodes in the network. And then the query issuing node tries to flood the query to each node in the network. While issuing the query to each node in the network the query issuing node tries to authenticate the authentication message held by each node and the authentication message came along with the query. After each node receiving the query the nodes that replies with data items with the k highest scores to two neighbour nodes. In addition to that each node includes, information on the reply message forwarding routes which consist of pairs of sender node and next node IDs, in its reply message. After the query-issuing node receives all the reply messages it can detect a DRA has been occurred by using the information came along a reply message route by using this attached information. After detecting the DRA, the query issuing node tries to identify the malicious nodes. The narrowing down and identification of malicious nodes are performing by making respective inquires. In the malicious node identification method, a query-issuing node that detects a DRA and narrows down the malicious node candidates by using the Send Route received from the detection algorithm and based on the received reply messages. From narrowing down each node tends to identify the neighbouring malicious nodes, but it is very hard to identify the malicious nodes which are far from it. Then each node shares the information or send notification message about the identified malicious node to its neighbouring ones. Then each node individually identifies malicious nodes using the shared information by using node grouping and malicious node identification. The node grouping is being done based on the information in the notification message received the nodes. After grouping, identification is being done based on the similarity of the information about the malicious node identified by the nodes in the each group. Based on the majority based judgment the malicious node is identifying. In this method the identified nodes are confirmed to be malicious by a number of groups equal to or greater than a certain limit. Since this method only identified the malicious nodes. Hence have to identify the liar nodes. So for that identifying the liar nodes from the group, the nodes which are not at all voted for at least any one of the malicious then that node is identified as liar node. Because each node is able to find malicious node from the group else it is protecting the malicious node. After finding the malicious nodes and the liar node again it will do the authentication method. That is at that time the query issuing node generates the authentication message and passes all the nodes except the malicious node. At the time of receiving query by each node it verifies the authentication message then at the part of malicious node it fails because it holds only the previous authentication message.After finding the malicious nodes and the liar node again it will do the authentication method.

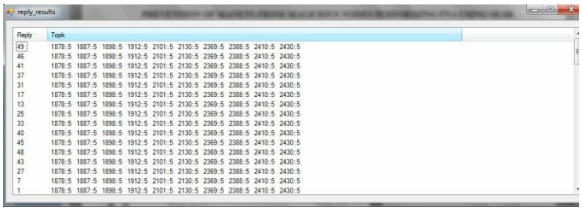
IV. EXPERMIENT RESULTS

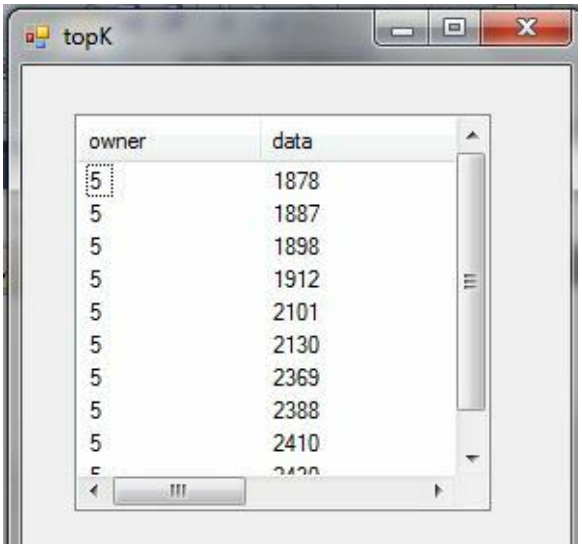


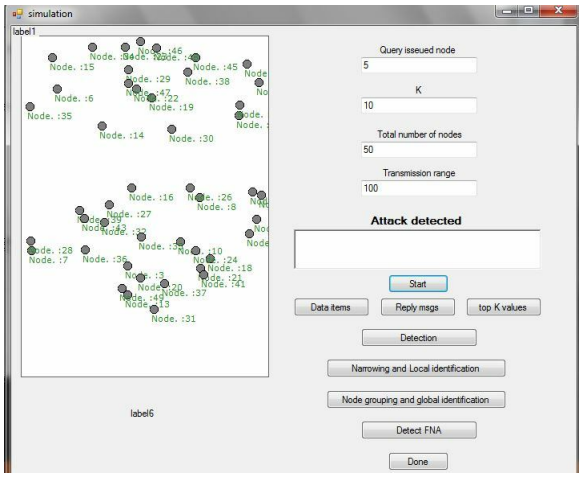












V. CONCLUSION

In this paper, we have proposed methods for top-k query processing and malicious node identification based on node grouping in MANETs. In order to maintain high accuracy of the query result and detect attacks, nodes reply with k data items with the highest score along multiple routes. After detecting attacks, the query-issuing node narrows down the malicious node candidates and then tries to identify the malicious nodes through message exchanges with other nodes. When multiple malicious nodes are present, the queryissuing node may not be able to identify all malicious nodes at a single query. It is effective for node to share the information about the identified malicious nodes with other nodes. In our method, each node divides all nodes into some groups by using the similarity of the information about the identified malicious nodes. Then, it identifies malicious nodes based on the information on the groups. In this paper, we did not address the issue of identification of liar nodes (LNs). As part of our future work, we plan to design a method to identify LNs, and also to design a message authentication method to prevent malicious nodes from performing FNAs.

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] S. Buchegger and J.-Y. Le Boudec, ‘‘Performance analysis of the CONFIDANT protocol,’’ in Proc. MobiHoc, 2002, pp. 226–236.

[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. 483–502, 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. 329–338.

[6] H. Chan, A. Perrig, and D. Song, ''Secure hierarchical in-network aggregation in sensor networks,'' in Proc. CCS, 2006, pp. 278–287.

[7] S. Chen, Y. Zhang, Q. Liu, and J. Feng, ''Dealing with dishonest recommendation: The trials in reputation management court,'' Ad Hoc Netw., vol. 10, no. 8, pp. 1603–1618, 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. 1000–1013, Jul. 2010.

[9] N. C. Fernandes, M. D. D. Moreira, and O. C. M. B. Duarte, ''A selforganized mechanism for thwarting malicious access in ad hoc networks,'' Proc. INFOCOM, 2010, pp. 266–270.

[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. 11–20.

[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. 12–23.

[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. 175–192, 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. 640–651.

[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. 536–550, 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. 338–346, 2007.

[16] 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.

[17] Z. Li and H. Shen, ''A hierarchical account-aided reputation management system for large-scale MANETs,'' in Proc. INFOCOM, Apr. 2011, pp. 909–917.

[18] X. Liu, J. Xu, and W. C. Lee, ''A cross pruning framework for top-k data collection in wireless sensor networks,'' in Proc. MDM, May 2010, pp. 157–166.

[19] W. Lou, W. Liu, and Y. Fang, ''SPREAD: Enhancing data confidentiality in mobile ad hoc networks,'' in Proc. INFOCOM, vol. 4. Mar. 2004, pp. 2404–2413.

[20] B. Malhotra, M. A. Nascimento, and I. Nikolaidis, ''Exact top-k queries in wireless sensor networks,'' IEEE Trans. Knowl. Data Eng., vol. 23, no. 10, pp. 1513–1525, Oct. 2011.

[21] S. Marti, T. J. Giuli, K. Lai, and