Indian J.Sci.Res. 17(2): 34-41, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

# MULTIPATH TRUST DETECTION ROUTING IN MANET

[1] Syeda Kausar Fatima, [2]Dr. Syed Abdul Sattar, [3]Dr. D. Srinivasa Rao
[1] Electronics and Communication Engineering, JNTUH, Hyderabad
[2] Nawab Shah Alam Khan College of Engineering and Technology, Hyderabad
[3] Electronics and Communication Engineering, JNTUH, Hyderabad

***Abstract -*** Mobile ad-hoc network is a self-organizing, infrastructure less network in which mobile nodes communicate using wireless channel. In MANET, the network created by the mobile nodes is dynamic in nature i.e. it is not confined to a particular topology because devices are free to move independently. Since there is no centralized node for monitoring in MANET routing path needs to be found dynamically. In this scheme we propose a novel multipath trust route approach to detect multiple malicious by implementing a route reply reverse tracing technique to help in achieving the stated goal. Proposed system helps us in defending against the multiple attack without any requirement of hardware and special detection node. This paper has been prepared keeping in mind that it needs to prove itself to be a valuable resource dealing with both the important core and the specialized security issues in this area.

***Keywords -*** MANET, Security, Trust Management in MANET, Route trust, Path trust

## I. Introduction

MOBILE ad hoc networks (MANETs) represent complex distributed systems that consist of wireless mobile nodes that can dynamically and freely self-organize into arbitrary and temporary ad hoc network topologies. This allows people and devices to seamlessly internetwork in areas where no pre-existing communication infrastructure exists, for example disaster recovery environments. The unique characteristics of MANETs, such as dynamic topology and resource constraint devices, pose a number of nontrivial challenges for efficient and lightweight security protocols design. Due to the lack of centralized identity management in MANETs and the requirement of a unique, distinct, and persistent identity per node for their security protocols to be viable, DoS attacks pose a serious threat to such networks.

### Active Attacks

Recently, there has been an increasing interest in mobile ad hoc networks (MANETs), which are composed solely of mobile nodes. Since such self-distributed networks do not require pre-existing base stations, they are expected to apply to various situations such as military affairs and rescue work in disaster sites. 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 who has the malicious node operates normally but the malicious node does various attacks (e.g. DoS attack such as blackhole attack).

An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication. We focus our work on network layer attacks such as Black hole attack and Denial of Service attack.

Black hole attack. The black hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrongdoing.

Denial of Service attack Denial of service (DoS) is another type of attack, where the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET. For example, consider the following Fig. 3. Assume a shortest path exists from S to X and C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial of service attack. Suppose S wishes to communicate with X and that S has an unexpired route to X in its route cache. S transmits a data packet toward X with the source route S --> A --> B --> M --> C --> D --> X contained in the packet's header. When M receives the packet, it can alter the source route in the packet's header,

[1]Corresponding Author

such as deleting D from the source route. Consequently, when C receives the altered packet, it attempts to forward the packet to X. Since X cannot hear C, the transmission is unsuccessful.

S ↔A↔ B↔ M ↔C↔ D↔ X

Figure 1: Denial of Service attack

A DoS attacker can cause damage to the ad hoc networks in several ways. For example, a Sybil attacker can disrupt location based on multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or node-disjoint paths. 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. In order to identify the malicious the novel Multiple Routes Trust Discovery processing method maintains query data item results, such as k highest scores along with multiple routes and reply route information enable to detect attacks. In addition, the route reply messages incorporate information about route and along with reply messages which are forwarded, so that the query-issuing node can distinguish the data items that properly belong to the message. The query issuing node narrows down the attack nodes based on the received message information and along with the request information on the data items, during identifying the malicious in a network and in this manner, the query-issuing node can discover the malicious node.

First we analyze an attack model of DoS, in such attacks the attack replaces data items with some fake data, we analyze suck kind of attacks to detect multiple malicious nodes using novel **Multiple Routes Trust Discovery** process. In order to determine multiple malicious nodes in a MANET we propose a novel **Multiple Routes Trust Discovery** which helps to identify malicious, the proposed model describes an attack model to determine route efficiency, we simulate this model to determine the accuracy and efficiency.

The remainder of this paper is organized as follows. In Section II we review the related work to the area of trust-based routing protocols. Section III provides problem definition. Section IV presents our novel trust-based routing protocol details the solution and describes the designed protocol. Section V shows the experimental study. Section VI we study the performance of our new protocol. Finally, Section VII concludes our work and provides future research directions.

## II. Related Work

Pirzada et al. define a trust mechanism [1] for a reactive routing protocol. They propose a model in which each node in an ad-hoc wireless environment maintains an evaluation procedure to reward or punish nodes in future collaborations. The evaluation generates trust values, which are based on transactions' history and the forwarding quality, that are shared with other nodes to choose a trust path. However, the proposal in [1] does not employ any measures to protect the evaluations conducted by the nodes and any malicious node can access these trust values and harm the routing functionality.

B. Chen, W. Liang et al. [2] have proposed methods to reduce energy consumption and traffic in unstructured P2Pnetworks or wireless sensor networks, by enabling nodes to filter unnecessary data items. However, these methods do not protect against DRA, and are unsuitable for use in MANETs, because they are not adapted to node mobility.

Raihana Ferdous et al [3] have proposed a Cluster head(s) selection algorithm based on an efficient trust model. This algorithm aims to elect trustworthy stable cluster head(s) that can provide secure communication via cooperative nodes. However the way the messages passed through may overload the Cluster head, creating a bottleneck due to additional message exchanges. Another possible limitation is the way that the message authentication between intermediate Cluster heads are treated, where there can be a delay in identifying a malicious neighboring node.

D. Amagata et al. [4] proposed a security of top-k queries in MANETs, in which data items are ordered according to a particular attribute score, and query-issuing nodes acquire the data items with the *k* highest scores in the network (the global top-k result). A large number of nodes participate in processing a top-k query in MANETs by both sending their own data items with high scores and relaying data items to the query-issuing node. Computational cost is high.

Although the above mentioned contributions provide important discussions that tackle various aspects of trust-based routing protocols, none of them has addressed the support of privacy in these protocols. We focus on this problem in this paper.

## III. Problem Definition

However, DoS attacks in MANETs have been actively studied for long years, and as a result, using existing techniques, such attacks can be exposed by the query-issuing node or intermediate nodes. Here, a remarkable characteristic of top-k query processing is that

the query-issuing node does not know the global top-k result beforehand.

MOBILE ad hoc networks (MANETs) represent complex distributed systems that consist of wireless mobile nodes that can dynamically and freely self-organize into arbitrary and temporary ad hoc network topologies. This allows people and devices to seamlessly internetwork in areas where no pre-existing communication infrastructure exists, for example disaster recovery environments. The unique characteristics of MANETs, such as dynamic topology and resource constraint devices, pose a number of nontrivial challenges for efficient and lightweight security protocols design. Due to the lack of centralized identity management in MANETs and the requirement of a unique, distinct, and persistent identity per node for their security protocols to be viable, Sybil attacks pose a serious threat to such networks.

## IV. Multiple Routes Trust Discovery or Path Trust

Multiple route discovery approach discovers the multiple trust routes to select highest trust path routing to compensate for the dynamic and unpredictable nature of ad hoc networks. We have designed a multipath trust routing protocol based on the trust information of the node involved. To calculate path trust, the RREQ and RREP packets are modified so that they contain the trust value of the node from which the packet is received. Both packets are changed because during route discovery a node transmits the RREQ packet by broadcasting. A node knows only the node from which the packet is received, not the node to which it is to be transmitted. Therefore, the RREQ packet is modified to incorporate the previous node's trust value and the RREP packet is modified to incorporate the next node's trust value. In initial process the route discovery process broadcast RREQ packet to corresponding neighbours. In order to identify the neigbhor node trust, the proposed protocol organizes the RREQ packet header with trust field, the trust field $p$, the $p$ represent trust path of each route,

$$RREQ : \{Srcid, Destid, Seqnum, TTL\}||p\ trust.$$

After broadcasting the RREQ packet, the source node sets a timer whose time period T is equal to the 1-way propagation delay and is calculated using formula given below:

To calculate route trust, the RREQ and RREP packets are modified so that they contain the trust value of the node from which the packet is received. Both packets are changed because during route discovery a node transmits the RREQ packet by broadcasting. A node knows only the node from which the packet is received, not the node to which it is to be transmitted. Therefore, the RREQ packet is modified to incorporate the previous node's trust value and the RREP packet is modified to incorporate the next node's trust value.

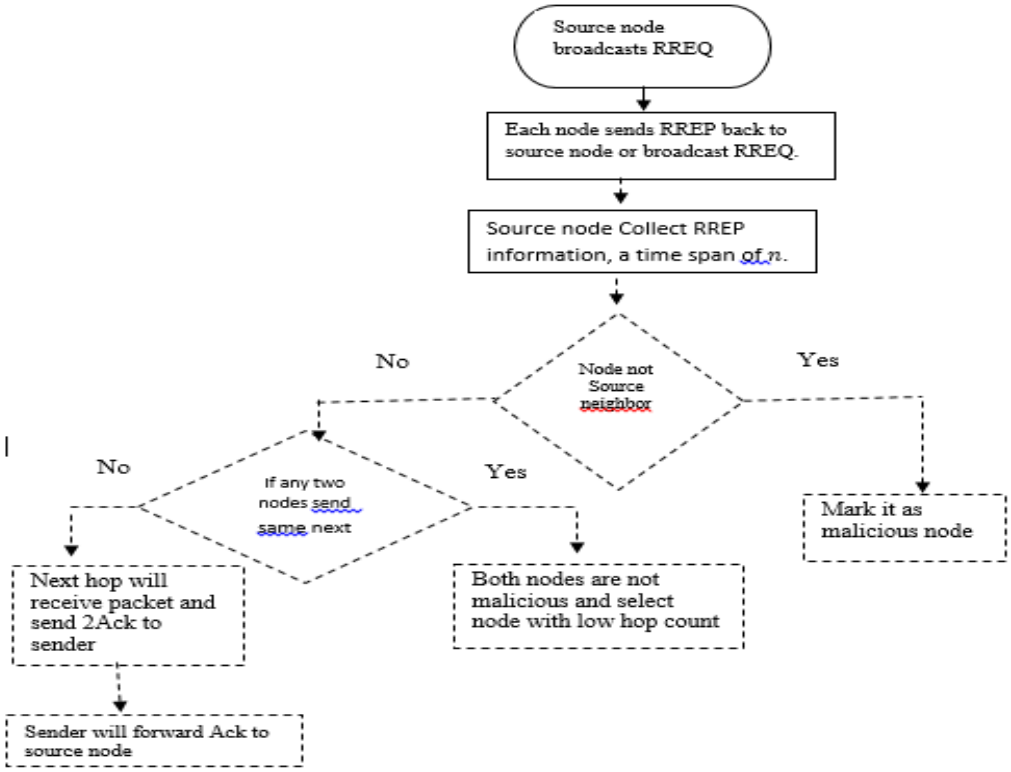


Figure2: Flowchart of the Proposed Scheme

### A. Route Trust Calculation

At a given time 0 t , we take a close look at node A and node B. Here we assume at certain time 0 t their velocity vectors are V1 and V2 respectively.

A as a stationary node and node B as a moving node, then we can calculate the relative velocity vector of node B to node A as $V = V_2 - V_1$ (1)

We take A as the reference node, from the view of node A, node B moves at a relative velocity V

A period time t, node B will travel out of the transmission range of node A, the relative movement track is $B \rightarrow B$

tdifs DCF interframe space

tbo backoff time

tdata delay for transmitting the data packet

tsifs short interframe space

tack delay of acknowledge

Te slot time in IEEE 802.11

tRTS delay of a RTS packet

tCTS delay of a CTS packet

L number of retries

B queue size

1. The delay of attempting to transmit a single packet over a link is

$$t_{packet} = T_c + t_{bo}$$

2. The delay associated with the transmission attempt, Tc, is equal to the delay associated with a successful transmission, Ts:

$$T_c = T_s = t + t_{data} + t_{siffs} + t_{ack}$$

3. The mean total delay for one single packet with L retries is then approximately

$$t_{packet-L} = L + 1 \,.\, T_c + \sum t_{bo}$$

4. The trust rate TRout out of queue when each packet has to be transmitted L times

$$TR_{out} = \min \left[ \frac{1}{t_{packet-L}} , R_{in} \right] = \min \left[ \frac{1}{(L+1).T_c + \sum t_{bo}} , R_{in} \right]$$

5. The total routing time is: $t_{rerouting} = t_d + t_e$

The RREP packet header is modified such that it contains two fields p trust and n trust in addition to other fields. The updated RREP is:

where p trust is assigned from the RREQ packet received at the destination and n trust is initialized to 0. It has the same significance as p trust in the RREQ packet and denotes the trust value of the path up to that node from the destination.

**Algorithm 1- RREQ Trust**

1: /* Receive a rreq message */

2: If node Nq receives a RREQ for the first time then

3: Store rreq path and hop counts as its Parent RREQ path

4: Compute the delay of single transmitting packet $t_{packet}$

5: Set RD for replying data items

6: /* Send the rreq message to neighbour nodes */

7: Add NNrreq, s node ID, $t_{packet}$ to the end of RREQ path

8: Send the rreq query to neighbor nodes

9: else

10: Compute the mean total delay $TR_{out}$ for one single packet with L retries and hop count as its Neighbor RREQ Query path

11: Store the node ID at the end of RREQ Query path as its neighbour

12: end if

In reply message algorithm, the replying node $Mr$ sends a reply message when its The mean total delay $t_{packet-L}$ time has passed. Here, REP signifies an reply message what's more, REP. Forwarding Route node signifies the sending routes list comprising of (Sender node ID, dest node ID), which means the set of sender and next node list, and $R$ means the most extreme number of reply messages to be re-sent. The replying node $Mr$ chooses the following node from its neighbouring nodes, which has the least hop count and least overlap between its re*lying node RREP path and the sender node's RREQ path

Algorithm 2- Sending a Reply Message

1: /* Sends a reply message after $t_{packet}$ time has elapsed */

2: /* Select a node to send a reply message */

3: **for** each Neighbor **do**

4: **if** Neighbor's hopCount is the minimum **then**

5: Insert Neighbor into DestNode

6: **end if**

7: **end for**

8: If DestNode > 1 **then**

9: Select a Neighbor whose Neighbor RREQ path least overlaps with the parent Query path as a DestNode

10: end if

11: Add the local top-k result to REP

12: **for** i = 0 to 1 do **do**

13: **if** i = 0 **then**

14: Add source node to received REP Forward node route.FR and send

**REP to source node**

15: **else if** i = 1 **then**

16: Add (Replying node Mr , DestNode) to received REP. Forwarder Route and send

**REP to DestNode**

17: **end if**

18: **end for**

19: /* Receive a reply message */

20: Send ACK to the sender node of REP

21: **if** before $t_{packet-L}$ **then**

22: Store REP

23: **else if** after $t_{packet-L}$ and reply node Mr receives a data item with higher score than with the kth-highest score among data items already sent **then**

24: Send REP including new local top-k result to parent node and DestNode

25: **end if**

26: /* Resend the reply message */

27: **if** Mr does not receive ACK from its parent by waiting time for retransmission and the number of retransmis sions < R **then**

28: Resend REP to parent

29: **else if** Mr does not receive ACK from DestNode by waiting time for retransmission and the number of retransmissions < R **then**

30: Resend REP to DestNode

31: **else if** the number of retransmissions > R **then**

32: /* Mr detects the disconnection of radio link */

33: **if** Mr has sent REP to all Neighbor **then**

34: Discard REP

35: **else if** Mr knows a Neighbor whose Neighbor Query path includes DestNode **then**

36: Send REP to the Neighbor

37: **else**

38: Select randomly a Neighbor among Neighbors which have not been selected yet

39: Send REP to the Neighbor

40: **end if**

41: **end if**

**B. Malicious Node Detection**

After the query-issuing node, *Mp*, receives all the reply messages, it detects a routing attacks according to Detection attack Algorithm. Each node calculates the local reputation scores of other nodes from correctness of received data, and computes the trust score $TR_{out}$ information in the network. Then, each node calculates the global reputation score from its own and received local trust scores. At last, it determines the node whose global score is lower than a threshold as the malicious nodes. The proposed method in which each node manages the reputation values of its neighbouring nodes in MANET.

Algorithm – Attack Detection

1: /* After the source node receives all reply messages */

2: INPUT: Top-k Result, REPs

3: OUTPUT: SendRoute

4: SendRoute← ∅ ;

5: **for** each REP **do**

6: **for** each Top-k Result **do**

7: **if** REP. forwarder route FR includes the node ID of a node processing

a data item in Top-k Result and REP.Data does not

include the data item **then**

8:Update a route from the node with the missing data

item to the query-issuing node into SendRoute

9: **end if**

10: **end for**

11: **end for**

12: **if** SendRoute ≠ ∅ ; **then**

13: Detect Attack

14: **end if**

**C. Malicious Node Identification**

The malicious node identification structured in three different stages such as 1. The initial query issuing node step; 2. The reverse tracing step; and 3. the shifted to reactive defense step, The first two steps are initial proactive defense steps, whereas the third step is a reactive defense step. A. Initial query node Step The goal of the query node phase is to entice a malicious node to send a reply RREP by sending the query node RREQ' that it has used to advertise itself as having the shortest path to the node that detains the packets that were converted. To achieve this goal, the following method is designed to generate the destination address of the query node RREQ'. The source node stochastically selects an adjacent node, i.e., nr , within its one-hop neighbourhood nodes and cooperates with this node by taking its address as the destination address of the query node RREQ'.

Reverse Tracing Step The reverse tracing step is used to detect the behaviors of malicious nodes through the route reply to the RREQ' message. If a malicious node has received the RREQ', it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the dubious path information and the temporarily trusted zone in the route.

## V. Experimental Study

In this section, the performance of the proposed ARDDT approach and the existing trustbased routing mechanism of TSCP, TEDR in MANET. The metrics used for the performance evaluation of the proposed ARDDT approach and existing approaches are PDR, throughput, average delay and energy consumption rates. The proposed system is simulated with the network simulator-2 (NS-2) with the simulation parameters of Table 1.

| No. of Nodes | 50,100,150 and 200. |
|---|---|
| Area Size | 1000 X 1000 |
| Mac | 802.11 |
| RadioRange | 250m |
| Simulation Time | 20 sec |
| Traffic Source | CBR |
| Packet Size | 512 |
| Receiving Power | 0.395 |
| Sending power | 0.660 |
| Idle Power | 0.035 |
| Initial Energy | 10.0 J |
| Attacks | Blackhole, Flooding Attacks |
| Data rate | 2 Mbps |

Table1 . Simulation Parameters

(1) Packet delivery ratio – data packets successfully delivered to the destination / data packets generated by the source,

(2) End-to-End Delay – the total time consumed that the data packet takes to reach from the source to destination vice versa,

(3) Routing packet overhead - the total number of control packets transmitted for each delivered data packet and

(4) Throughput – the average number of data packets transmitted per unit of time.

(5) Number of malicious detection rate: The total number of malicious predicted and detection is estimated

## VI. Simulation Results

The performance of ARDDT protocol is analyzed and the observations are made with respect to the parameters of packet delivery ratio, End-to-End Delay, routing packet overhead and throughput. Fig. 5 demonstrates the performance of ARDDT protocol and TSCP at different moving speeds of mobile node with the traffic load of 4 packets/second

We evaluate mainly the performance according to the following metrics.

**Average Packet Delivery Ratio:** It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

**Average Routing overhead:** It is the average number of routing packets by nodes.

**Delay:** It is the time taken by the packets to reach the receiver.

**Average Throughput:** It is the amount of successful message delivery over a node

### A. Results and Discussion

The performance of MRDT protocol is analyzed and the observations are made with respect to the parameters of packet delivery ratio, End-to-End Delay, energy consumption and throughput. Fig. 2 demonstrates the performance of MRDT protocol and Top-k at different mobile nodes

According to Fig. 1, MRDT has the better packet delivery ratio than Top-k under different malicious nodes. Fig. 2 shows that end to end delay between the proposed MRDT protocol and Top-k, according to the fig-2, Top-k end-to-end delay rate increased when there are more number of attack nodes.

According to Fig. 3, MRDT performs slightly better throughput than TOP-k. The throughput of the both protocols decreases as the node speed increases.

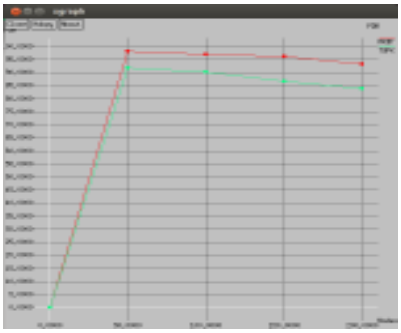

Figure 1- PDR- MRDT vs TOP-K

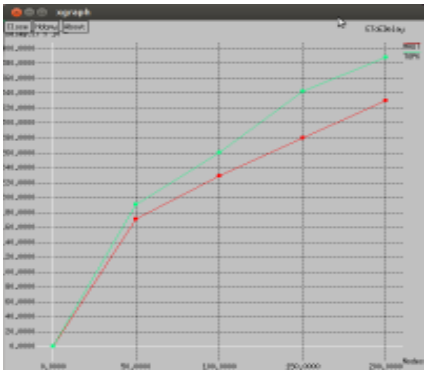

Figure 2- End-to-End Delay- MRDT vs TOP-K

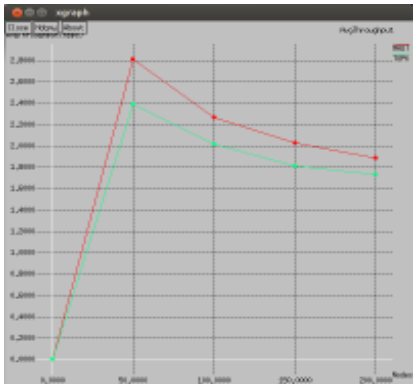

Figure 3- Average Throughput

Figure 4 Energy Consumption

## VII. Conclusion

In this paper, we have analyzed the security threats an ad-hoc network faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of an ad-hoc networks require high degree of security on the other hand, ad-hoc network are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. In this system, the methods for top-k query processing and malicious node identification based on node grouping in MANETs is proposed. 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 malicious node and then tries to identify the malicious nodes through message exchanges with other nodes. 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 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.

## References

[1] A.A. Pirzada, A. Datta, and C. McDonald, “Trust Based Routing for Ad- Hoc Wireless Networks,” In *Proceedings of IEEE International Conference on Networks (ICON'04)*, pp. 326-330, 2004.

[2] 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.

[3] Raihana Ferdous, Vallipuram Muthukkumarasamy and Elankayer Sithirasenan, “Trust-based Cluster head Selection Algorithm for Mobile Ad hoc Networks”, Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on. IEEE, 2011.

[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.-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.

[6] S. Buchegger and J.-Y. Le Boudec, ``Performance analysis of the CONFIDANT protocol," in *Proc. MobiHoc*, 2002, pp. 226_236.

[7] 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.

[8] S. Hashmi and J. Brooke, "Toward Sybil resistant authentication in mobile ad hoc networks," in Proc. 4th Int. Conf. Emerging Security Inform., Syst. Technol., 2010, pp. 17–24.[7] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," IEEE Trans. Veh. Technol., vol. 59, no. 5, pp. 2418–2434, Jun. 2010.

[9] M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within VANET," Int. J. Netw. Security, vol. 8, pp. 322–333, May 2009.

[10] 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.

[11] 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.

[12] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ," Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.