Malicious Node Identification in MANETs based on False Information

S. Afrose and S. Venkatesh Babu

1PG scholar, Department of CSE Christian College of Engineering and Technology, Oddanchatram, Dindigul, India.
2Asst. Professor, Department of CSE Christian College of Engineering and Technology, Oddanchatram, Dindigul, India.

Received 18 January 2017; Accepted 22 March 2017; Available online 28 March 2017

Address For Correspondence:
S. Afrose, PG scholar, Department of CSE Christian College of Engineering and Technology, Oddanchatram, Dindigul, India.
E-mail: afrosefrs@gmail.com

Copyright © 2017 by authors and American-Eurasian Network for ScientificInformation (AENSI Publication).
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/

ABSTRACT

The query processing in mobile adhoc network (MANETs) is identifies the malicious node attack by using an approach of top k query processing. A malicious node can inject wrong routing information creating false routing able entries thus hardening the end-to-end MANET communications. In this paper an effort is formed to get the nodes that are malicious in nature the recent work of attack is possible one in Data Replacement Attack (DRA) and another one is False Notification Attack. DRA attack replaces the necessary Knowledge items with redundant information items and FNA comprises the normal node as malicious node. The proposed method detects these attacks by using score values in top k query processing. In top k query processing, node reply with data items and high score values based on this value query issue node identify the data replacement attack in network. After detecting the attack based on the malicious node information query issue node group the node in order to identify the false notification attack in network. This method improves the accuracy of top k result for malicious node identification in MANET.

KEYWORDS: MANET, Top-k, query, NA, Security, Authentication.

INTRODUCTION

Manet is formed dynamically by an autonomous system of mobile nodes that are connected via wireless links. It has no existing fixed infrastructure or centralized administration. Mobile nodes are free to move randomly. Each should forward traffic unrelated to its own use, and thus be a router. The first challenge in building a Manet is mobilization every device to endlessly maintain the data needed to properly route traffic. Such networks could operate by themselves or is also connected to the larger net. They’ll contain one or multiple and completely different transceivers between nodes. This ends up in a extremely dynamic, autonomous topology.

MANETs are a form of Wireless spontaneous network that typically includes a routable networking setting on high of a Link Layer spontaneous network. In a MANET, nodes inside one another’s wireless transmission vary will communicate directly; but, nodes outside one another’s vary got to trust another nodes to relay messages. This network is required in military application and emergency rescue operations. But lowly MANETs have entered with the areas of play, sensing, and conferencing, cooperative and distributed computing.

Since such self-distributed networks don’t need pre-existing base stations, they’re expected to use to varied things like military affairs and rescue add disaster sites. Since every node has poor resources the communication information measure and also the battery lifetime of mobile nodes square measure restricted. The nodes can use a top-k query process technique to induce the data of the complete network. A node can issue a query this query can moves kind one node to a different node supported the routing algorithm. Each node can contribute their
answer and also the items are ordered consistent with their attribute score and also the query-issuing node can get the information with the k highest score in the network. In this environment malicious owing to an attack from outside the network, the malicious node tries to disrupt the operations of the system.

The malicious activity is of 2 fold the primary case the malicious nodes can deploy data Replacement Attack (DRA), the second is false Notification Attack (FNA). The network with malicious nodes can still operate usually the user of the network can still operate while not the data of the presence of the malicious node. The malicious node can attempt to implement Denial of Service attack and blocks the query process within the network. In the case of top-kquery processing to identify the top-k objects is scoring all objects based on some scoring function. An object score acts as a valuation for that object according to its characteristics (e.g., price and size of house objects in a real estate database, or color and texture of images in a multimedia database). Data objects are usually evaluated by multiple scoring predicates that contribute to the total object score. Due to increase in analysis activity within the space of top-k query process, the impact of economical top-k process is turning into evident in an increasing variety of applications [1].

The malicious node tries to disrupt the query provision node by denying the worldwide top-k query result for long period with being detected this is called as denial of service attack. The DoS attack is being studied by several research worker for long term therefore its several techniques as counter measures. In data replacement attack (DRA) the query supplying node won't get the world top-k query score earlier therefore the malicious node can replaces high-score value with its own low score value. The query provision node can believe that the information it receive could be a correct world top-k query result and it's difficult to find the attack. DRAs attack are stronger than alternative the other ancient attacks therefore some specific form of mechanism is have to be compelled to overcome the DRA attack and harder to find than other traditional forms of attack, therefore some specific mechanism for defensive DRAs are needed. In this paper, we tend to propose top-k query process at the side of the strategy to observe DRA attack in MANETs.

In the query process to keep up accuracy of the top-k query score and notice the attacks, the replay information item contains results and additionally includes the path data using which the query provision node will confirm the replay path and assure that results are from authentic nodes. The query provision node will slander right down to the malicious node using the received path data and may request to suspend the information item once more. During this approach, the query-issuing node will determine the malicious node [1]. But in typical network there’ll be additional variety of malicious nodes are obtainable within the network it’s troublesome to spot them using a single query message. However the planned methodology is intended to spot the malicious node in AN economical approach within which if a node realize its near node to be an malicious one and this inform is shared with all different normal nodes with within the network during this approach all the nodes can have global image regarding the malicious nodes.

During this case, someday a standard node will send false data for this sort of attack we tend to planned a replacement methodology that finds false notification attack (FNA). Each nodes within the network shares regarding the malicious node they need classified supported the path and data with this information the normal the traditional the conventional nodes will determine the attacks even though the malicious nodes mixes the data as that of normal node.

The remaining section of this paper is organized as follows: Section II reviews some of the existing works Section III provides the detailed description for the overall propose system. Section IV presents the performance results of the proposed system. Finally, this paper is concluded in Section V.

I. Related Work:

This section presents some of the existing works related In networks wherever aggregation is wont to get the result on device network the main objective is to classify those node that are trusted node that contribute to the aggregation calculation. In [2] a secure hierarchical in-network aggregation in wont to establish the misdemeanor node and stop them from collaborating within the aggregation calculation. In unintended networks [3], to get only the required information items effectively every mobile node retrieves information items employing a top-k query. so as to scale back the traffic with high accuracy of the query result, every node can send a bar graph information [4] supported the query to query provision node with this bar graph it’s straightforward to search out the best score value. A routing table primarily based methodology is planned in [5] to accomplish high accuracy in query process using top-k query. The top-k query process is performed in 2 sections [6] in section one the query provision node can collect all the query result and in second phase it’ll resolve the result with highest score primarily based on threshold calculation. In two-tier device network [7] master slave design is employed. During which the master node collects information from device node and answers the query from the network owner during this methodology the master node should bea trusted node. In co-operative Peer-to-peer (P2P) there’s a chance that one peer might cheat the other peer and propagate malicious code or some they don’t work [8].
II. Proposed Method:

This proposes top-k query processing and malicious node identification methods against DRAs and FNA attack in MANETs. In the top-k query processing method, in order to maintain accuracy of query result and detect attacks, nodes reply with data items and k highest scores along with multiple routes. Moreover, to enable detection of DRA, 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 retrieve to the message. In the malicious node identification method, the query-issuing node first narrows down the malicious nodes, using information in the received message, and then requests information on the data items sent by these nodes.

A. Network Creation:

The Network is made with 60 mobile nodes without any base station as self-distributed nodes. Every node is assigned with a unique identification number and quality pattern is random. The node will exchange information packets and management packets as outlined by the protocol

B. System Model:

The network consists of mobile node is described by N= wherever n is that the total variety of nodes within the network and that they are known exploitation the number NID=, Where m=n, the information within the network is denoted as D=, wherever k is that the total range information of knowledge of information and every information is known by exploitation data symbol Di, where i=k. The algorithmic program works in distributed environment therefore every node needs to exchange additional data with the near node in order that they exchange information packet often therefore to avoid intermediate nodes to not modify the information content public key encryption methodology is employed. every node is aware of the general public key of alternative nodes therefore information are send by encrypting with the general public key of the receiving node. so as to reduce the computation the query message are not encrypted.

C. Data Replacement Attack:

DRA attack means that original information replaced by the some unwanted information that causes the unreliable communication of Manet. Data replacement attack introduce by the malicious node that replaces the received information items with unnecessary information items. DRA attack is strong attack; it’s very tough to observe then different attacks in MANETS. The cases for difficult to detection the DRA attacks like initial case the node has only one neighboring node and send the reply message on single path. Second malicious node reply with the traditional message, as a result of if alternative nodes recognize the malicious node it'll be neglected. The nodes are sent the normal message. Depending on network topologies malicious node could not replaces the information in networks

The node within the network will generate a query and send it to the all the nodes to induce a desired value [9]. Allow us to assume a node want the person detail with a specific people with high pressure level, low vision, this demand is generated as query and propagated towards the network. Allow us to think about m be the query provision node and Mq be the node that replay for the query with its own score value this can be the conventional scenario, the case won't stay for durable. In some scenario a malicious node could capture the node and induce its own low score value to form the aggregation to be invalid.

The query kind query provision node have {a query question |a question} id and therefore the id of the query provision node (Qid, Nid) the query goes to nearby node and this node can include its score price and its identification (SVi, Nid).There will be 2 list one is to store the replay Score price List (SVL) and therefore the second is Replay Path price (RPV) that store the trail of the query propagation message or replay message. The query can take multiple path within the network.

The query path is outlined because the variety of hop count that is calculated supported the network size and therefore the radio vary between nodes. The waiting time for the replay is defined because the operate of variety of hop count between the source node and therefore the replay node and therefore the most size of the network together with the waiting time of query at every node.

\[ \text{Replay\_WT} = (\text{Net\_Size} - D\_SR) \times \text{WaitTime} \]

Where Replay\_WT is that the replay waiting time for a query provision node and Net\_Size is that the size of the network and D\_SR the amount of hops between the source node and current replay node, the waiting time is that the time that a query takes to be processed at each node. The nodes can sends back the replay with its own identifier (Source node ID), and replay route (Dest node ID) [9], a list of data items that containing the score values.The reply message includes 2 lists, Score value List (Contains all the collected score values) and also the second list is Replay Path value (Contains all the nodes that as referred to as forward nodes id), If the Replay Path value includes a node id however there's no date within the Score value List this states that some replacement is finished that's Data Replacement Attack is taken place. The nodes can compare the score with the neighbor to find the attacks.

Here we tend to observe the DRA attack by using the highest k query result. In top k query process, query
issue node sends the query message (query id with needed information items) to the nodes through the multiple
path in networks. Node that have the requested data items those are send the reply message (data items, score
values and route data) supported this information the query issue node establish the data replacement attack in
MANETs.
We can observe the DRA attack only reply message from multiple path in networks. Here our planned
methodology query issue node sends the high score value with needed data items to the nodes on the multiple
ways. The nodes are reply data items with score values based on score value detect the DRA attack by compares
results with neighbor node reply message, supported these message we will detect the data replacement attack in
Manet.
D. False Notification Attack:
FNA attack means that some cases malicious node send the fake data i.e. normal node as malicious node. FNA attack additionally called liar node attack as a result of the malicious node replies with the normal messages.
The nodes are classified with some similar properties. Every group can have a group in-charge that is
elected by Nodes highest ID. If some node within any cluster identifies an attack supported the algorithm one
it'll report the malicious node id to is group in-charge and this data is shared with all alternative group in-
charge within the network. every group in-charge can try and adapt weather the node is malicious node or lire
node (LN). Where LN are traditional node which can contribute a false value. No value to top-K query. The
LN nodes can update the score value in Score_Value_List thus it's not a malicious node, to verify this query
issue node can send a request to the current LN node to send its score value. Then the values are compared with
the values collected from replay messages if the values are of in greater variation the LN nodes are categorized.
Here we tend to detect the FNA attack, when detecting DRA attack the query issue node tries to identify
the malicious node in network, that send the malicious node information by the route information in reply
message.
Here we detect the FNA attack with low score values i.e. zero score value. Node that has the zero score
value we tend to determine that node as FNA attacker node as a result of in Manet all normal node score values
should be high, normal node value does not get zero based on this we detect the FNA attack.
E. Top K Query Processing:
In the top-K query process methodology, so as to maintain accuracy of query result and detect attacks, nodes
reply with information items with k highest scores on multiple routes. In the top-K query process methodology,
1st query issue node sends the query message with query node id and needed data items in multiple routes in
networks then the node sends the reply message with requested data items, score value and route data supported
this data query issue node detect the attack in networks when detecting the attack node group based on
malicious node information.
III. Performance Analysis:
This section presents the performance results of the proposed. The results are analyzed and evaluated in
terms of
- Confidentiality.
- Integrity.
- Availability.
- Energy consumption performance.
- Prevention techniques.
A. Confidentiality:
Only the supposed receivers should be able to interpret the transmitted information. As an example is
using digital signature mechanism.
B. Integrity:
Data shouldn't change throughout the transmission method, and data send should be same with the data
receive.
C. Availability:
Network services should be obtainable all the time after they are required.
D. Energy Consumption and Performance:
Develop a communication protocol in Manet. Routing protocol needs to have a best performance to
improve the standard of communication, i.e. communication delay, packet delivery rate, throughput and
overhead. Routing protocol should have a minimum delay, most delivery rate and minimum overhead during the communication method. Many causes of the network performance degradation are external attack and fast ever-changing of the configuration

E. Resource consumption:
By injecting further data packets into the Ad Hoc network restricted resources such as bandwidth and perhaps battery power are consumed for no reason. Even additional resources may well be consumed by injecting additional control packets since these would possibly cause further computation. Also, the different nodes would possibly forward management information as it comes in leading to even a lot of resource consumption. It refers to intense the communication bandwidth within the network or storage space at individual nodes. For instance, an internal offender could consume the network bandwidth by either forming a loop within the network.

F. Prevention Techniques:
There are some of the prevention techniques which once applied will result in the secure and also the better results for the transferring of the data from supply to the destination.

G. Secure Routing:
In the routing protocols authentication techniques helps to avoid several of the attacks represented above. The nodes desire to participate in routing method guarantee that the nodes are authenticated. Trusted network components can behave consistent with the protocol rules. During this means unauthorized nodes can prevent from collaborating within the network and interference of occurring routing attacks.

H. Authentication:
It may be based mostly either on public key or symmetric cryptography. Within the former case, nodes issue digital signatures related to the routing messages. Signatures may be verified by the other node, providing a secure proof of the identity of the sender.

RESULTS AND DISCUSSION

The proposed ideas are implemented in NS2. The mobile nodes are selected with the subsequent parameters.

once the malicious nodes are known and removed and conjointly once the malicious nodes are present the query result accuracy is low as shown in figure 2. The figure 3 shows the traffic flow once the queries are issued within the network and it's compared with the attack and while not attack.

The traffic is high once there's a malicious nodes within the network since they contribute false data within the network this lead the normal node to send a lot of query to settle down on correct result.

Table 1: NodeDetails

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation area</td>
<td>1500mx1500m</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>200</td>
</tr>
<tr>
<td>Mobility model</td>
<td>Randomwaypoint</td>
</tr>
<tr>
<td>Node communication range</td>
<td>250m</td>
</tr>
<tr>
<td>Speed</td>
<td>5-25m/s</td>
</tr>
<tr>
<td>Routing protocols</td>
<td>AWCBR</td>
</tr>
<tr>
<td>MAC</td>
<td>802.11</td>
</tr>
<tr>
<td>Traffic source model</td>
<td>ConstantBitRate (CBR)</td>
</tr>
<tr>
<td>Simulation time</td>
<td>500 seconds</td>
</tr>
</tbody>
</table>
Fig. 1: Query Result Accuracy

Fig. 2: Packet Drop Ratio

Conclusion:

The proposed work is intended to produce secure data sharing among the nodes present in Mobile Ad-hoc Networks. As per the previous work the query-issuing node was not in a position to determine attacker node if present in massive numbers. Such a drawback is overcome by this technique within which we determine attacker’s nodes present in the network supported broadcasting the queries. We particularly determine the foremost harmful attacks like data Replacement attack and False Notification attack. On identifying these 2 differing kinds of attacks we maintain secure data transmission among nodes. On identifying such attacks we improve the performance of our network

REFERENCES