Top-k Query Processing and Malicious Node Identification Based on Node Grouping in MANETs

Dr.T.Ranganayaki
Associate Professor, Department of Computer Science,
Erode Arts and Science College (Autonomous), Erode, Tamil Nadu, India.
D.Gobika
M.Phil Research Scholar, Department of Computer Science,
Erode Arts and Science College (Autonomous), Erode, Tamil Nadu, India.

Abstract- Autonomous wireless nodes without fixed infrastructure are connected to construct the Mobile Ad-hoc Networks (MANET). The MANETs are build and used in the military, commercial and disaster management operations. The data provider node provides its data to other wireless nodes. The shared data values are transferred with reference to the query received from other nodes. All the request and response elements are passed through the path nodes. The query request and reply are transmitted with different routing schemes. The query request and reply operations are carried out to access the data values under the data providers. The query value is broadcasted to all the nodes in the MANET. The top-k data elements are produced as reply for the queried node through different routes. The reply data can be changed in the intermediate node. The malicious data modification activity is referred as Data Replacement Attack (DRA). Query reply verification is carried out to detect the malicious node discovery process. The clustering process groups the neighbor nodes with resource and proximity information. The malicious node detection is carried out in cluster level with local and global verification schemes. The malicious node information is broadcasted as notification to all nodes. The MANET data query scheme is composed with data sharing and security features. Cluster construction and malicious node detection operations are built with data security. The malicious node discovery process is improved with liar node and False Notification Attack (FNA) discovery operations. The Message Authentication Code (MAC) is prepared with confidentiality and integrity verification schemes. The malicious node operations are controlled using the Message Authentication Code. The RSA algorithm, Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) are used for the data confidentiality and integrity verification process.

Keywords- RSA,SHA,MAC,DRA,AES,MANET.

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of wireless mobile devices with restricted broadcast range and resources. Recently, there has been an increasing interest in mobile ad hoc network (MANET), which is constructed by only 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, since each node has poor resources (i.e., the communication bandwidth and the battery life of mobile nodes are limited), it is effective to retrieve only the necessary data items using top-k query, in which data items are ordered according to a particular attribute score, and 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 mayexecute a variety of attacks. The mobile ad-hoc networks (MANET) are temporary wireless networks.

Duplicate detection is based on entropy algorithm for discovering a finding by using dis-similarity calculation. This is a new solution for duplication problem. It employs entropy formula to calculate the homogeneity of a data for continuous attributes McCallum et al (2000) and Barrodaleand Ericson (1980). Gain is computed to estimate the gain produced by a split over an attribute. The quality of the result and the performance of the algorithm have been compared. The rest of the paper is organized as follows. In Section 2, the related studies rendering the fusion methods with brief review. The characteristics of ENTROPY are described in detail and the proposed method ENTROPY is established in detail way in Section 3. In Section 4, the characteristics of INFORMATION GAIN(IG) is described . In Section5 algorithm description of with grouping and without grouping is analyzed. In section 6, the performance analysis is shown. Finally, a conclusion is given in section 7.

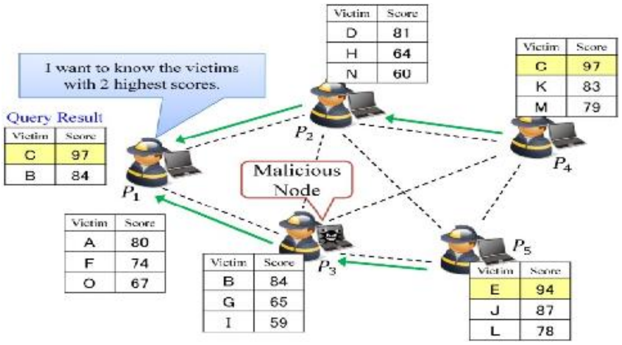

Fig.1. Example top-k query in a MANET.

The mobile nodes with self-adaptive and self-management features are grouped to construct the Mobile Ad-hoc Network (MANET). Data values in a mobile node can be shared with all the nodes in the network. The MANET data transmission operations are carried out without the infrastructure dependency. Military and disaster management operations are efficiently handled with the support of the mobile nodes. The mobile nodes are used to collect and distribute the victim details in the rescue operations. The query processing schemes are applied to fetch the victim details with user submitted query values. The MANET applications are designed with the consideration of the energy and bandwidth parameters.

In the worm hole attack an attacker selectively forward all the data by making a special short circuit in the ad hoc network. This type of attack can capture most of the control over the network. In this paper, we present the details of the Cluster and Reputation based Cooperative Malicious node Detection and Removal (CRCMD&R) scheme to mitigate the adverse effects of misbehaving nodes.

Mobile ad hoc networks (MANETs) are communication network that consist entirely of wireless nodes, placed together without prior planning. Due to the limited transmitter range of mobile nodes, the nodes must rely on one another in forwarding a packet [1]. Along with the advances on MANETs and their open media nature, increases the demand for secure routing.

Current routing protocols are more vulnerable to malicious participants. Such participants could silently drops or corrupt some or all of the data packets instead of forwarding them properly. This type of participant is called malicious node and attack is called malicious packet dropping [2]. It further leads to some special kinds of attacks may disrupt the communication entirely. Other routing attacks are grey hole attack [4],[5] , worm hole attack[6].

In Black hole attack the attacker sends out wrong routing information within the network. It can setup a path to some destination via itself & when the actual data packets get there they are simply dropped. A special case of the black hole attack is grey hole attack. In this the adversary selectively drops some kind of packets.

2. RELATED WORKS

An innovative detection system is considered to help identify the man-in-the-middle and wormhole opponents. A simple modification to the wireless MAC protocol is carried out to portray the survival of a rival performing a frame-relaying attack. This alteration has wide applications and is suitable for MANETs, infrastructure and wireless mesh networks. With a better rate of detection, minus false positives and negligible bandwidth loss, this method proves to be the most efficient.

A collusion attack model called the optimized link state routing (OLSR) protocol is proposed against one of the four standard routing protocols for MANETs. The first attacker creates a duplicate link and allows the exploit the packet so that the packets can route themselves. Based on experiments, it was discovered that the attack can have destructive effects on the OLSR MANET. With the help of information from two hop neighbors, the attack is identified after an examination. Different kinds of flooding attacks, recognition of these attacks, and mechanisms to prevent them are analyzed. As far as flooding attacks are concerned, detection methods are categorized based on irregularity or behavior, specification and knowledge. The span of this analysis is to formulate a better, secure identification and prevention system for flooding attacks in future [3].

It is imperative to appreciate the vulnerability of the protocol against a wormhole attack. An examination is done on performance parameters such as end-to-end delay, throughput, traffic received, utilization and network load. The OLSR and AODV are affected more by wormhole attacks if the number of nodes and route requests are correspondingly higher In comparison, the AODV is more susceptible to wormhole attacks than the OLSR. Investigations have proved this conclusively through experiments and mathematical results. When more than one attacker exists in the network, the MANET application that uses the proactive routing protocol is more trusted than the one that uses the reactive one.

The packet dropping attack is observed. A security protocol has been proposed for identifying the means of packet dropping nodes in MANET and, in that way, redirecting a secure routing course from the source node to the target node, preventing the entry of malicious nodes. The result obtained has been simulated with ns-2 and evaluated with the AODV and modified AODV security system [7].

Different kinds of attacks over MANET have to be summed up and related with examining sleep-deficiency attacks. One of the several danger theory intrusion identification algorithms, particularly the dendritic cell algorithm (DCA), is used to identify sleep deficiency attacks over MANET. The DCA is blocked in an estimated mobile dendritic cell algorithm known as the MDCA. The MDCA has to be carried out by each node in MANET for identifying attacks in surrounding areas devoid of any means of mobile communication [8].

From the viewpoint of the AODV protocol, a method for recognizing and averting sinkhole problems and their consequences is discussed. Applying this method, the performance of the AODV is assessed relatively, and it is confirmed that the AODV efficiency is improved substantially. An observation is carried out on the deviation in the values of a range of performance metrics such as the PDR, end-to-end delay, throughput and packet loss. The performance of the AODVs takes a backseat when many nodes are attacked [9].

Rushing attacks are new and potent attacks against on demand ad hoc network routing protocols, and the origin and outcome of rushing attacks on dynamic source routing (DSR) protocols is talked about. The impact of rushing attacks is scrutinized, taking into consideration fundamental mechanisms such as route discovery and route maintenance [10].

A new traffic analysis attack known as the least squares disclosure attack (LSDA), aiming at familiar MANET routing plans, is considered in order to negotiate obscurity in communication between mobile ad hoc networks.

Based on perflow, the LSDA de-anonymizes network communication by using the traffic distribution disclosed by existing solutions. On linear limitation, traffic disclosure is represented as a least squares problem. It is demonstrated that the resolution can de-anonymize network flows with high precision [12].

How a rival implants a malicious node in the network by using a colluding attack and, at the same time, hiding its uniqueness from other valid nodes is discussed. The attack is termed the colluding injected attack (CIA). As the infused nodes work collectively, a harsh attack is generated in the network, the idea being to create a conflict at a random node which, in turn, makes the attacked node unable to receive or transmit packets. Therefore, any node in the same area can wrongly report this node as a malicious node. Simulation results show that detecting methods in the past might have been misguided by colluding injected attacks [11].

The rescue operations are initiated and managed with reference to the data maintained under the data provider nodes. The data request is broadcasted as a top-k query value. The query reply is prepared with top-k items using the victim and score information. The query reply values are modified with the Data Replacement Attacks initiated by the malicious nodes. Malicious nodes exist, for example, the data items in the top-k result are sent back along a single route, and thus are vulnerable to DRA. Drawbacks in Existing System are Liar node identification is not provided, False Notification Attack discovery is not supported, Data security is not provided and Malicious node control mechanism is not available. Current system does notaddresstheissueofidentification of liar nodes (LN s). So, the proposed method is to design a method to identify LN s, and also to design a message authentication method to prevent malicious nodes from performingFNAs.

3. MANET Query Process and Attack Discovery Schemes

Recently, there has been an increasing interest in mobile ad hoc network (MANET), which is constructed by only 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, since each node has poor resources, it is effective to retrieve only the necessary data items using top-k query, in which data items are ordered according to a particular attribute score, and the query-issuing node acquires the data items with k highest scores in the network. 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.

Let us 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. 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. 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. 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 with unnecessary yet proper 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.

An example of performing a top-k query in a MANETs, where a rescue worker in a disaster site acquires data items with 2 highest scores. Let us assume that the mobile node held by the rescue worker at P3 becomes a malicious node, and it replaces the received highest score data item whose score is 94, with its own lower-score data item whose score is 84. Therefore, the node held by the rescue worker at P1, who issues a top-k query, cannot acquire the data item whose score is 94, and it cannot know the node at P3 performed a DRA.

In this paper, we propose top-k query processing and malicious node identification methods again DRAs 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 with k highest scores along 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 belong to the message. In the malicious node identification method, the query-issuing node first narrows down the malicious node candidates, using information in the received message, 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 there are multiple malicious nodes in the network, it is difficult to identify all the malicious nodes in a single query. By using our methods, nodes are likely to identify the malicious nodes which are near their own location, while they hardly identify the malicious nodes which are far from their own location. Therefore, in order to quickly identify more malicious nodes, it is effective to share the information about the identified malicious nodes with other nodes. In this case, a malicious node may declare fake information that claims normal nodes as the malicious nodes. We need some method to correctly identify the malicious nodes against FNAs.

Therefore, in our malicious node identification method, after nodes share the malicious node identification information, each node divides all nodes into some groups based on the similarity of the information. Then, the node determines the final judgment of malicious nodes based on the judgment result of each group. In our method, even if malicious nodes claim that normal nodes are the malicious nodes, there is a decisive difference in the nature of the information possessed by normal and malicious nodes concerning the identified malicious nodes, and therefore, the normal nodes can easily identify the malicious nodes. Furthermore, even if malicious nodes mix the correct information on malicious nodes identified by other normal nodes with their fake information, in order to increase their similarity with normal nodes, the normal nodes in the same group will nonetheless certainly identify the malicious nodes, but not normal nodes. Thus, the information from the malicious nodes can be removed and there is little influence of FNAs.

4. Security Challenges in MANET Data Sharing Applications

Data provider node maintains the data items for query process. The query-issuing node foods a query over the entire network. The K-data items are replied with highest score values with multiple routes. Data Replacement Attacks are initiated to change the data items in query reply. The query-issuing node tries to detect attacks from the information attached to the reply messages. The malicious nodes are identified with the message communication with other nodes. Multiple malicious nodes cannot be identified using a single query value. Malicious node information is shared with other nodes. All the nodes are divided into groups. Malicious nodes are identified with the information collected from the groups. The attacks are discovered with reply route details. Local and global identification methods are adapted for the malicious node detection process. The following security challenges are identified from the current MANET data sharing methods. Liar node identification is not provided. False Notification Attack discovery is not supported. Data security is not provided. Malicious node control mechanism is not available.

The Data values are shared between the nodes under the Mobile Ad-hoc Network environment. The system detects Data Replacement Attacks (DRA) initiated by the malicious nodes and Clustering methods are adapted to detect Liar nodes and False Notification Attacks. So, the Data security is provided in the message communication process.

5. MANET Data Sharing with Security and Malicious Node Discovery

The mobile ad-hoc networks are constructed to support infrastructure less communication operations. The data values are transferred through the intermediate nodes. The emergency and rescue operations are carried out with the query process models. The victim information is managed under the MANET nodes. The query values are released to identify the victims with high injury conditions. The score values are used to discover the top-k data values. The top-k query processing results are redirected to the queried node through the intermediate nodes. The data values are updated with reference to the score values. The data replacement attacks are raised by the malicious nodes. The attack resistant query processing framework is build to support the query process with attack control and discovery mechanism. Cluster based attack discovery scheme is used in the system. Local and global level attack discovery operations are adapted in the system. The message authentication schemes are integrated into the system to control the malicious node activities.

The mobile ad-hoc network query processing system is divided into five major modules. They are Clustering process, Data Providers, Query Processing, Malicious Node Discovery and Message Authentication Process. The clustering process module is build to setup the MANET and node grouping process. The data provider module manages the shared data values. The query submission process is build to submit the query for the MANET nodes. The attacks and its sources are discovered under the malicious node detection process. The message authentication process is designed to protect the query request and response operations.

The mobile ad-hoc network is constructed with user parameters. User parameters are used to construct the mobile ad-hoc networks. The nodes are classified into two categories such as data provider and node. Clustering process is initiated to group the MANET nodes. Coverage and resource details are used in the clustering process. The cluster head manages the nodes under the group. The data provider node shares the data values to other nodes. The data provider maintains the victim details. The score values are used to indicate the victim severity levels. Provider list shows the data providers with victim count details. Victim ID and score details are listed in the victim data details. The data values are distributed with reference to the query values. The query values are passed through the intermediate nodes.

The top-k query processing scheme is used in the system. The data values are filtered with reference o the score values. The sender node releases the query value through the intermediate nodes with multiple routes. The responses are prepared by the data provider node. The query response is passed through the intermediate nodes with different route values. The data values are updated with the score values of the intermediate nods. The query responses are collected and summarized by the queried node. The malicious node discovery process is used to detect the attacker nodes. Data replacement attacks are discover with response verification under different nodes. Local and global discovery models are used in the system. The malicious node identification process is carried out with the following steps. They are forwarding a Query, Sending a Reply Message, Detection of Attack and Narrowing down the Malicious, Identification of a Malicious Node, Node Grouping and Global Identification. The liar node identification and false notification attack discovery operations are also carried out under the malicious node discovery process.

The message authentication process is applied to protect the query responses I the top-k query processing under the mobile ad-hoc network environment. The data security schemes are also provided in the query processing operations. Cryptography and digital signature methods are adapted for the message authentication process. The RSA, Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) are used in the message authentication process. The query responses are attached and verified with a Message Authentication Code (MAC). The data replacement is discovered in the integrity verification process. The malicious node attacks are controlled in the message authentication process.

6. CONCLUSION

The Top – K queries are used to retrieve data items from MANET nodes. Malicious nodes replace the necessary data with unnecessary data values. Node grouping method is applied to perform the top-K queries with malicious node identification process. Liar Node and False Notification Attacks are detected with message authentication schemes. Data values are shared between the nodes under the Mobile Adhoc Network environment. The system detects Data Replacement Attacks (DRA) initiated by the malicious nodes. Clustering methods are adapted to detect Liar nodes and False Notification Attacks. Data security is provided in the message communication process.The Data values are shared between the nodes under the Mobile Ad-hoc Network environment. The system detects Data Replacement Attacks (DRA) initiated by the malicious nodes and Clustering methods are adapted to detect Liar nodes and False Notification Attacks. So, the Data security is provided in the message communication process.

REFERENCES

[1] Saurabh Sharma and Dr. Sapna Gambhir, “CRCMD&R: Cluster and Reputation based Cooperative Malicious Node Detection & Removal Scheme in MANETs”, 11th International Conference on Intelligent Systems and Control (ISCO), 2017.

[2] G. S. Mamatha and S. C. Sharma "Analyzing the MANET Variaitons, Challenges, Capacity and Protocol Issues" international Journal 0/ Computer Science & Engineering Survey (fJCSES) , voU, no.1 , pp. 14-21 , August 2010.

[3] Mohil, Nitin, and KantaDhankhar. "Survey of Detection and Prevention Mechanism for Flooding Attacks in MANETs." International Journal of Research in Advent Technology 2.5, May 2014.

[4] Saurabh Gupta, Subrat Kar, S Dharmaraja, "BAAP: Black hole Attack Avoidance Protocol for Wireless Network," in Proc. iCCCT'j j , 2011 , p.468-473 .

[5] Rutvij H. Ihaveri, Sankita J. Patel and Devesh C. linwala, "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad hoc Networks," in Proc. ACCT '12, 2012, p. 556-560.

[6] Saurabh Gupta, Subrat Kar, S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet," in Proc. JJT'll, 2011 , p. 226-231.

[7] Madhurikkha, S.; Sabitha, R., "Defending against packet dropping attack using DRI & cross checking mechanism in MANET," Information Communication and Embedded Systems (ICICES), 2013 International Conference on, vol., no., pp.260,264, 21-22 Feb. 2013

[8] MahaAbdelhaq, Rosilah Hassan, Mahamod Ismail, RaedAlsaqour, DaudIsraf” “Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm”International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085).

[9] Gandhewar, N.; Patel, R., "Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network," Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on , vol., no., pp.714,718, 3-5 Nov. 2012.

[10] Kumar, Sushant, and BibhudattaSahoo. "Effect of Rushing Attack on DSR in wireless Mobile Ad hoc Network." Proceedings of the 2010 ACM Workshop on Wireless Security. Vol. 1. No. 11. 2010.

[11] Kandah, Farah, Yashaswi Singh, and Chonggang Wang. "Colluding injected attack in mobile ad-hoc networks." Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on. IEEE, 2011.

[12] Qin, Yang, and Dijiang Huang. "Least Squares Disclosure Attack in Mobile Ad Hoc Networks." Communications (ICC), 2011 IEEE International Conference on. IEEE, 2011.