ISSN:2348-2079

Volume-5 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Attack Resistant Query Processing Framework for MANET

Ms. D. Janaranjani, Ms. Kasthuri, Ms. S. Malar and Mr. E. Kavin Kumar, Final Year BTech (IT).,
Mrs. R. Maheswari, ME, AP (Sr. Gr), Department of Information Technology,
Velalar College of Engineering and Technology., Erode, Tamilnadu, India
janaranjani2013@gmail.com

Abstract - The mobile ad-hoc networks (MANET) are temporary wireless networks. Emergency and rescue operations are supported with MANET environment. Data values in a mobile node can be shared with all the nodes in the network. The query values are issued for the shared data access. The intermediate nodes retransmit the query and its response values to other nodes. Different routing schemes can be adapted to transfer the query and response values. All the MANET applications are designed with the consideration of the limited battery power and bandwidth levels.

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 can not be identified using a single query value. Malicious node information are 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 MANET data sharing scheme is designed to access the shared data with security. The mobile ad-hoc network nodes are grouped as clusters with reference to its coverage and resource levels. Cluster based malicious node discovery process is performed in the system. Liar node and False Notification Attack (FNA) discovery mechanisms are integrated with the system. Message authentication methods are integrated to control malicious nodes. Data confidentiality and integrity verification schemes are combined in the message authentication mechanism.

1. Introduction

A mobile ad-hoc network is a kind of wireless ad-hoc network and is a self-configuring network of mobile routers connected by wireless links – the union of which forms an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

Mobile ad-hoc networks became a popular subject for research as laptops and 802.11/Wi-Fi wireless networking became widespread in the mid- to late 1990s. Many of the academic researches evaluate protocols and abilities assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other and usually with nodes sending data at a constant rate. Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol and other measures. The Children's Machine One Laptop per Child program hopes to develop a cheap laptop for mass distribution to developing countries for education. The laptops will use ad-hoc wireless mesh networking to develop their own communications network out of the box.

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief

efforts and military networks. Such network scenarios cannot rely on centralized and organized connectivity and can be conceived as applications of Mobile Ad-Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes they, i.e., routing functionality will be incorporated into mobile nodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling and routing. Determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

2. Related Work

Reputation systems can be classified into two categories: direct observation [1] and indirect observation [3], [2] methods. In the former, nodes independently assess their neighbors' reputations based on their direct interactions. It reduces the complexity of reputation management and achieves performance comparable to the approaches requiring reputation exchanges in a certain scenario. In the latter, nodes periodically share the reputation information they observed with others. The works in [4], [7] use techniques of *watchdog* and *pathrater*. *Watchdog* in a node promiscuously listens to the transmission of the next node in the path in order to detect misbehaviors. *Pathrater* in a node keeps the rating of other nodes to avoid interaction with uncooperative nodes in the transmission. CONFIDANT [5] detects uncooperative nodes and informs other nodes of observed misbehavior. Wu and Khosla [6] proposed an authentication mechanism to authenticate reputation messages in order to prevent a selfish node from playing tricks to benefit itself. Anantvalee and Wu [10] introduced a new type of nodes called suspicious nodes, which will be further investigated to see if they tend to behave selfishly by two reputation threshold(s).

Buchegger *et al.* proposed a Bayesian prediction mechanism to increase system robustness to falsely disseminated information. They also investigated the effect of using rumors on the detection time of misbehaving nodes and the robustness of reputation systems against wrong accusations. Mundinger *et al.* [2] built a stochastic process to formulate the behavior of the nodes in the system and derived a mean ordinary differential equation for misreport detection. Luo *et al.* [3] built a fuzzy logic model to deal with the uncertainty and tolerance of imprecise data inputs. Price systems provide incentives for cooperation by using micro payment. Buttyan *et al.* proposed two payment models: packet purse model, in which a source node pays relay nodes by storing virtual credits in the packet head, and packet trade model, in which a relay node buys packets from the previous node and sells them to the next node in the path. In the credit-based system in [10], when a node forwards a message, it keeps a receipt and uploads it to the credit clearance service for credits.

Crowcrof *et al.* proposed a traffic price approach, in which the compensation of message

forwarding depends not only on the energy consumption of the transmission but also on the congestion level of the relaying node. A node chooses a route to a destination with the minimum route compensation. Janzadeh *et al.* [9] proposed a price-based cooperation mechanism that utilizes hash chains to defend against cheating behavior. As described, individual reputation and price systems are not insufficiently efficient and effective. These deficiencies are confirmed in our previous work [6] which used game theory to investigate the underlying cooperation incentives of both systems. ARM resolves the problems in the individual system and greatly enhances the system efficiency and effectiveness by coordinately integrating the two systems through a DHT-based infrastructure.

3. Malicious Node Identification in Top-K Query Process Under MANETs

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 [7]. 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. 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 [8]. 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 *P*3 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 *P*1, who issues a top-k query, cannot acquire the data item whose score is 94, and it cannot know the node at *P*3 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 (*false notification attack* (*FNA*)).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. Our contributions are as follows:

- We describe a new attack model, DRA, in which a malicious node replaces necessary data items with unnecessary ones, and we analyze the effects of such an attack on top-k query processing when there are multiple malicious nodes in the networks.
- We propose methods for processing top-k queries and for identifying malicious nodes against a DRA in MANETs.
- We describe an attack model, FNA, in which a malicious node sends fake information that claims some normal nodes as malicious nodes, and we evaluate the effects of such an attack.
- We verify that our proposed methods can achieve high accuracy of the query result and identify malicious nodes, through extensive simulations that take into account physical layer effects in the networks.

4. Problem Statement

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 can not be identified using a single query value. Malicious node information are 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 problems are identified from the current top-k query processing schemes in MANET environment.

- 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

5. Attack Resistant Query Processing Framework

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 are 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.

5.1. Clustering Process

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.

5.2. Data Providers

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.

5.3. Query Processing

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.

5.4. Malicious Node Discovery

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, 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.

5.5. Message Authentication 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. Data Security Scheme

The data security is ensured with Cryptography and digital signature techniques. The RSA and Advanced Encryptio Standard (AES) algorithms are used for the data confidentiality purpose. The integrity verification is carried out using the Secure Hash

Algorithm (SHA). The message authentication codes are build with the key and signature values.

6.1. RSA Algorithm

The domain name service sensitive attributes are secured using the RSA algorithm. The Rivert, Shamir, Adelman (RSA) scheme is a block cipher in which the Plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits or 309 decimal digits.

Key Generation

Select p,q p and q both prime , $p \neq q$

Calculate $n = p \times q$

Calculate $\phi(n)=(p-1)(q-1)$

Select integer e $\gcd(\phi(n),e) = 1; 1 < e < \phi(n)$

Calculate d $d = e^{-1} \bmod \phi(n)$

Public key $KU = \{e, n\}$

Private key $KR = \{d, n\}$

Encryption

Plaintext $M < n$

Cipher text $C = M^e \pmod n$

Decryption

Cipher text C

Plaintext $M = C^d \pmod n$

6.2. Secure Hashing Algorithm

The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS), and may refer to:-

A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. Cryptographic weaknesses were discovered in SHA-1, and the standard was no longer approved for most cryptographic uses after 2010.

7. Conclusion

Top – K queries are used to retrieve data items from MANET nodes. Malicious nodes replaces 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.

References

[1] D. Amagata and Nishio, ``A robust routing method for top-k queries in mobile ad hoc networks," in Proc. MDM, Jun. 2013.

[2] J. Mundinger and J. Le Boudec. Analysis of a reputation system for mobile ad-hoc networks with liars. Performance Evaluation, 2008.

[3] J. Luo, X. Liu, and M. Fan. A trust model based on fuzzy recommendation for mobile ad-hoc networks. Computer Network, 2009.

[4] Ze Li and Haiying Shen, "A Hierarchical Account-aided Reputation Management System for Large-Scale MANETs", IEEE, 2011

[5] T. Anantvalee and J. Wu. Reputation-based system for encouraging the cooperation of nodes in mobile ad hoc networks. In ICC, 2007.

[6] Z. Li and H. Shen. Analysis of a hybrid reputation management system for mobile ad hoc networks. In Proc. of ICCCN, 2009.

[7] S. Chen, Y. Zhang, and J. Feng, ``Dealing with dishonest recommendation: The trials in reputation management court," Ad Hoc Netw., , Nov. 2012.

[8] T. Tsuda, Y. Komai and S. Nishio, ``Top-k query processing and malicious node identication against data replacement attack in MANETs," in Proc. MDM, Jul. 2014.

[9] H. Janzadeh and K. Fayazbakhsh and M. Dehghan and M. S. Fallah. A secure credit-based cooperation stimulating mechanism for MANETs using hash chains. Elservier, Future Generation Comput. Sys., 2009.

[10] T. Anantvalee and J. Wu. Reputation-based system for encouraging the cooperation nodes in mobile ad hoc networks. In Proc. of ICC, 2007.