Scrutiny International Multidiciplinary
Free Research Journal
(SIMFRJ)

Providing security in mobile social network using the concept of keyadmin

M. I. Peter Shiyam[1] and J. Stephy Christina[2]

[1]Assistant Professor, Department of Computer Science and Engineering, DMI Engineering College, Aralvaimozhi Tamil Nadu
[2]PG Scholar, Department of Computer Science and Engineering, DMI Engineering college, Aralvaimozhi, India

Corresponding author

M. I. Peter Shiyam,
Assistant Professor,
Department of Computer Science and Engineering,
DMI Engineering College,
Aralvaimozhi, Tamilnadu,
India.

Abstract

A mobile social network (MSN) is one kind of delay tolerant networks (DTN) composes to the mobile nodes can be move around and share information to other mobile nodes towards the carried shortest distance in wireless communication networks. In heterogeneous network spread the all messages at different locations at frequently but it gives the expected and average delay delivery of the messages. At the same time the messages are not sending by secure manner. The proposal techniques used in Key Admin and shortest distance algorithm. The source node communicates with KeyAdmin, and it generates the keys in source address and destination address. The KeyAdmin communicate with all KeyAdmin's and send to the key. The destination will be reaches the message and it will get the key for KeyAdmin. The KeyAdmin verifies the destination address and gives the key for decrypt the message. The shortest distance algorithm will be calculated in nearest mobile node distance. So it gives more efficient and high performance for minimum delay delivery of the packets and authentication of the each message.

***Key words:** Delay tolerant network, heterogeneous, Delay, Security, KeyAdmin, Key.*

Introduction

Mobile social networks (MSNs) are composed of mobile users that move around and use their carried wireless communication devices to share information via online social network services, such as Facebook, Twitter, etc. Recently, the short-distance communication model has also been adopted by encountered mobile users in MSNs to share information, such as multimedia, large-size files, etc., at a low cost. Such MSNs can be seen as a special kind of delay tolerant network (DTN). Fig. 1 shows a simple example. Like other DTNs, there are generally no stable end-to-end delivery paths in an MSN, due to the mobility of nodes. Therefore, delivering messages is a challenging issue. Many routing algorithms that are based on store-carry-and-forward schemes have been proposed to address this issue. The existing algorithms can simply be divided into two categories.

One category is novel zero-knowledge routing algorithms, which do not require any prior knowledge on the contact probabilities or social characteristics of nodes. The typical algorithms include Epidemic and Spray& Wait. Epidemic spreads messages to each encountered node through the flooding strategy. To avoid producing too many message copies, Epidemic in the real implementation generally limits the maximum number of copies. Spray& Wait also limits the number of copies. Moreover, it adopts a binary splitting method to spread copies into the network until one message holder encounters the destination. Both of the algorithms assume that all nodes just randomly walk in a given area, and that nodes visit all locations in a uniformly random way.

In fact, MSNs have social characteristics; compared to traditional DTNs. Nodes in an MSN generally visit some locations frequently, while visiting other locations less frequently, due to their different interests. The nodes that frequently visit the same location will form a community with a common interest, as shown in Fig. 1. The location is seen as the home of the community. Many mobility models from real MSN traces have captured this characteristic of skewed location visiting preferences.

Moreover, each community home (or simply, home) in real traces can support a real throw box, a device that can locally store and forward messages, or can let the nodes that are visiting it act as virtual throw boxes. Such social characteristics can be utilized to guide message deliveries so as to improve the routing performance. Another category consist of extend home spread algorithm, requires the objective is to minimize the expected delay of delivering each message from its source to its destination, while the copies of each message are no more than a given threshold. The algorithm consists of three phases. In the first phase, the source spreads copies quickly to homes. In the second phase, the homes that have received more than one copy spread the message to other homes and mobile nodes (or simply nodes). Then, in the third phase, the destination fetches the message from any encountered message holder, which is either a mobile node or a home that has message copies. This algorithm makes use of the unbalanced location visiting characteristic and uses homes as special message holders. Thus, it can achieve a better performance than existing zero-knowledge routing algorithms. The main contributions are summarized as follows:

1) We first propose the HS algorithm for homogeneous MSNs, in which all mobile nodes share all community homes. Moreover, we show that HS is optimal in homogeneous MSNs when the inter-meeting time between any two nodes and between a node and a home follows independent and identical exponential distributions.
2) We also extend the HS algorithm to the heterogeneous MSNs, in which mobile nodes might have different community homes. We show that HS can still achieve good message delivery performance in the heterogeneous MSNs.
3) We construct a continuous Markov chain to calculate the expected delivery delay of HS and derive an upper bound. Moreover, we calculate the number of message copies required to bound the expected delivery delay to a given threshold.

It conducts extensive simulations on a synthetic MSN trace to evaluate HS. The results show that HS significantly outperforms the existing zero-knowledge multi-copy routing algorithms, including Epidemic with a given number of copies, and Spray& Wait.

Network Model

We consider a typical MSN that is composed of a number of mobile nodes and many locations. Each node frequently visits a few locations, called community homes or homes, while the other locations, called normal locations, are visited less frequently.

Each node might have multiple homes. Many real MSNs follow this unbalanced-visiting characteristic. Moreover, we assume that each home has a throwbox that can locally store and forward messages. Many real applications can support throwboxes, such as the roadside units in vehicular ad hoc networks, the base stations in delay tolerant networks, etc.,. Even though there are no real throwboxes in some homes, we can let the nodes that are visiting these homes act as the virtual throwboxes.

If a node that acts as a virtual throwbox wants to leave the home, it can handoff its messages to another node in this home. In fact, it has pointed out that virtual throwboxes will only result in a little bit of performance degradation, compared to real throw boxes. In addition, we assume that the throw box in each home has enough cache space to store messages from visited mobile nodes. This is reasonable since a real throw box is generally equipped with a large cache. If a virtual throw box has limited cache, we can let multiple nodes that are visiting the home act as the virtual throw boxes at the same time, so that they can also provide a large cache together.

Network Problem

In this paper, we consider two MSN settings: the homogeneous setting and the heterogeneous setting. In heterogeneous network spread the all messages at different locations at frequently but it gives the expected and average delay delivery of the messages. At the same time the messages are not sending by secure manner.

HS: Heterogeneous msns

In this section, we extend the HS algorithm from the homogeneous setting to the heterogeneous setting, where each node might have a different home set, but all of them will form the overlapped home set H. As a zero-knowledge routing algorithm, the source in HS does not know which homes the destination is related to. Without loss of generality, the source treats every home as a potential home of destination. Then, the objective is still to spread the message copies to each home. If there are extra copies, it will spread them to other mobile nodes.

The Homing Phase

In the homing phase, the source tries to send the message to the homes first. If the source encounters other nodes before it reaches a home, it will give some of its copies to the encountered node, and will let the node jointly send the copies to homes. The more nodes that the message copies are sent to before reaching homes, the smaller the delay of the next two phases will be. Thus, the source needs to spread the copies to as many other nodes as possible before they reach the homes. To this end, we adopt the following homing scheme:

Definition 1. (Binary Homing Scheme). Each message holder sends all of its copies to the first (visited) home. If the message holder encounters another node before it visits a home, it binary splits the copies between them.

The Spreading Phase

In the spreading phase, the homes which have more than one copy spread their extra copies to other homes and nodes. Then, we adopt the following spreading scheme.

Definition 2 (1-Spreading Scheme). Each home l_i 2Hspreads a copy to each node in the same home until only one copy remains, so that l_i 2Hafter the spreading. If such a node with one copy later visits another home l_j 2H, the node sends the copy to that home, so that l_j 2Hafter the visit.

The Fetching Phase

In the fetching phase, the destination just fetches the message once it encounters a message holder. This message holder might be in the homing phase or the spreading phase. The worst case is that all message copies have finished the spreading phase before the destination gets the message.

The Extended HS

First, we consider the homing phase. Since the nodes in the heterogeneous setting have different home sets, the expected delays for them to visit a home will be different. In general, the more homes a node has, the more quickly the node will send its copies to a home. Thus, when two nodes that have copies meet, the node with more homes should hold more copies, so as to minimize the average delay for these copies to be delivered to the homes. On the other hand, in order to minimize the delays of the next two phases, we also need to let these copies spread to as many homes as possible. In terms of this objective, each pair of encountered nodes should equally split their copies. Thus, there is a tradeoff in the splitting of copies. To this end, we adopt the following homing scheme in HS.

Methodology

Shortest distance algorithm

The shortest distance algorithm can be used for the calculating the distance, because the mobile nodes are moving and it located for different places. The mobile nodes are frequently visited some different locations and it shares an information towards the carried shortest distance in wireless communication networks.

The algorithm can be only for the shortest distances nearest and longest distance mobile nodes. That are providing at the more less than time for finding at the source to destination mobile nodes, because that are selecting at manually. The algorithm can be represented by the way in Pythagoras theorem for calculating the distance at three mobile nodes, and all mobile nodes are compared at these mobile node distances.

Algorithm: Shortest distance algorithm

Pseudocode

```
int a,b,c;
for(i=0;i<n;i++)
{
```

```
for(j=0;j<n;j++)
{
sqr a=i*i;
sqr b=j*j;
distance c=sqrrt((sqr a)+(sqr b));
}
}
return c;
```

Keyadmin technique

The KeyAdmin technique can be used for the security purposes. So it works on generating and share the key in other KeyAdmin's. The selecting source mobile node communicate with the KeyAdmin, and the KeyAdmin generated the key for selecting source node and selecting destination address.The KeyAdmin shares or communicate with all other KeyAdmin's for authentication purpose.

The selecting source mobile node share or send messages or information through the selecting destination mobile node. The selecting destination mobile node requires for the key in KeyAdmin. But the KeyAdmin verifies the selecting destination address because the key is generated by the selecting destination address and the keyAdmin stores the selecting destination address.

Algorithm: KeyAdmin technique
Pseudocode

The selecting source mobile node encrypted the message in the form,

$e = kab$
$d \Xi e^{-1} \pmod k$

The KeyAdmin verifies the selecting destination mobile node address is represented by,

Plain text, $M < n$
For encryption, $C = M^e \bmod n$

The selecting destination node decrypted the message in the form,

For decryption, $M = C^d \bmod n$

Where,

M= Message Size
C= Cipher Text
e= Encryption key
d= Decryption key
n= number of mobile nodes.
a= selected source node address.
b= selected destination node address.
k= key.

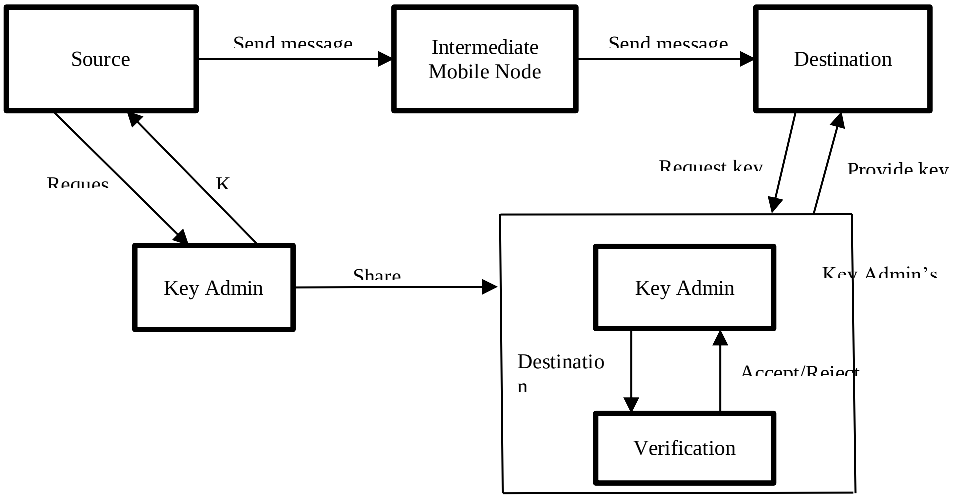
In this way message are shared by the heterogeneous network of selecting source mobile node and selecting destination mobile nodes. Then it provides the communication between at authentication purposes.

Those are getting the more efficient and secure in the authentication protocols. That are gives the more efficient results by the time of communication process at the selecting mobile nodes in manually.

Architectural diagram

In the architectural diagram represented by the communication between through the selected source mobile node and KeyAdmin and selected destination mobile nodes.

Architectural diagram



The source mobile node requested the keyAdmin and it generated by the key in source address and destination address. The source mobile node send to message in encryption form in destination mobile node. The KeyAdmin can be shared by the other KeyAdmin's. The destination mobile node requires the key for decrypt the message. The KeyAdmin verifies the destination mobile node address and it gives the key.

Results

The results are showed by initialize the mobile node and the shortest path, selected source mobile node and selected destination mobile node. The computation process granted by the selecting source and destination node at this time. So other process are granted at the particular communication.

Conclusion

It concludes that analysis and simulation results show the homes play an important role in the message spreading process. The shortest distance algorithm gives the minimum delay delivery and it gives efficient process. The KeyAdmin algorithm gives the authentication process and more security of the communication channel.

Reference

M. Xiao, J. Wu, and L. Huang, "Community-aware opportunistic routing in mobile social networks," IEEE Trans. Comput., vol. PP, no. 99, pp. 1–14, 2013.

T. Ning, Z. Yang, H. Wu, and Z. Han, "Self-interest-driven incentives for ad dissemination in autonomous mobile social networks," in Proc. IEEE Conf. Comput. Commun., 2013, pp. 2310– 2318.

L. Guo, C. Zhang, H. Yue, and Y. Fang, "A privacy-preserving social-assisted mobile content dissemination scheme in DTNs," in Proc. IEEE Conf. Comput. Commun., 2013, pp. 2301–2309.