IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

A Position Based Opportunistic Routing Protocol for Secured Data Transfer In MANET

[1]Dhivya.R, [2]Divya.L, [3]Aswini.R, [4]R.Evangelin Hema Mariya.
[1,2&3]Final Year-CSE, Kingston Engineering College, Vellore, Tamilnadu.
[4]Assistant Professor, CSE, Kingston Engineering College, Vellore, Tamilnadu.

Abstract

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. It is a multi hop, self configuring, and infrastructure-less network of mobile devices connected by wireless. In MANET, each device is free to move independently in any direction. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. The problem in MANET is to deliver the data packets in highly dynamic network in a reliable and secure manner. The existing routing protocols like DSR, DSDV are susceptible to node mobility (Movement of nodes). So, in this paper we propose an efficient Position-based Opportunistic Routing (POR) protocol. The design of POR is based on Geographic Routing and Opportunistic Forwarding, which transfers the data packet based on the location of the destination. The concept of in-the-air backup reduces the latency and duplicate relaying caused by local reroute. To increase the level of security we also encrypt the data, before transmission. For encryption of data we use RC4 algorithm which converts original text into cipher text. Using RC4 algorithm encryption time is reduced and it also fastest algorithm compared to other algorithms.

Keywords: Forwarding candidate, Geographic Routing, Mobile Ad-hoc NETwork, Private key, Stream cipher,

1. Introduction

Ad-Hoc networks are infrastructure-less networks, made up of mobile nodes, which are using their neighbors as a means of communication with other nodes in the network. A source node that needs to communicate with a destination node uses either a direct link or a multi hop route to reach the latter. Ad-hoc networks change their topology, expressed by the node connectivity, over time, as the nodes change their position in space.[5]Routing schemes of mobile ad-hoc networks can be crudely divided into two groups: topology based routing, and position-based routing. Topology based routing uses existing information in the network about links; it includes table driven protocols, such as DSDV and CGSR, on demand protocols, such as AODV, DSR, and more.

Position-based routing, on the other hand, is based on the nodes position in space and their local neighboring node position. Traditional topology-based MANET routing protocols (e.g., DSDV, AODV, DSR[1]) are quite susceptible to node mobility. One of the main reasons is due to the predetermination of an end-to-end route before data transmission. Once the path breaks, data packets will get lost or be delayed for a long time until the reconstruction of the route, causing transmission interruption. Geographic routing (GR) uses location information to forward data packets, in a hop-by-hop routing fashion. No end-to-end routes need to be maintained, leading to GR's high efficiency and scalability.

2. Related Work

Josh Broch, David A. Maltz David B. Johnson Yih-Chun Hu, Jorjeta Jetcheva [1] proposed the results of a derailed packet-level simulation comparing four multi-hop wireless ad hoc network routing protocols that cover a range of design choices: DSDV,DSR and AODV. The position of a mobile node can be calculated as a function of time, and is used by the radio propagation model to calculate the propagation delay from one node to another and to determine the power level of a received signal at each mobile node.

Brad Karp, H. T. Kung [2] discussed The two dominant factors in the scaling of a routing algorithm, the rate of change of the topology and the number of routers in the routing domain. Under GPSR, packets are marked by their originator with their destinations' locations. As a result, a forwarding node can make a locally optimal, greedy choice in choosing a packet's next hop.

Eric Rozner Jayesh Seshadri Yogita Ashok Mehta Lili Qiu [3] proposed a Simple Opportunistic Adaptive Routing protocol (SOAR) to explicitly support multiple simultaneous flows in wireless mesh networks. SOAR incorporates the following four major components to achieve high throughput and

fairness: (i) adaptive forwarding path selection to leverage path diversity while minimizing duplicate transmissions, (ii) priority timer-based forwarding to let only the best forwarding node forward the packet, (iii) local loss recovery to efficiently detect and retransmit lost packets, and (iv) adaptive rate control to determine an appropriate sending rate according to the current network conditions.

Dazhi Chen, Jing Deng, Pramod K. Varshney [4] proposed a Contention-based Geographic Forwarding (CGF) technique. Accordingly, CGF mainly consists of the following components: 1) A predefined forwarding area and nodes that reside in the area become next-hop candidate nodes; 2) a distributed contention arbitration and resolution scheme to effectively establish a single next-hop node in the forwarding area; 3) a next-hop node selection criterion so as to attain the desired network performance efficiently; and 4) an effective mechanism to handle voids. A high-level model of CGF is established.

Noa Arad, Yuval Shavitt [5] defines that many of the problems of position-based routing originate from the fact that the shape of the network is unknown a priori, and it is dynamically changing due to node mobility. GPSR [15], for example, switches from recovery mode back to greedy mode when the current node is closer to the destination than the node who switched to perimeter mode. However, there is no guarantee that this node, or the next one, will not be another concave node, a local maximum on the perimeter face.

3. Proposed Method

3.1. Position-Based Opportunistic Routing

Opportunistic routing (OR) takes advantages of the spatial diversity and broadcast nature of wireless networks to combat the time-varying links by involving multiple neighboring nodes (forwarding candidates) for each packet relay. Firstly, we study geographic opportunistic routing (GOR), a variant of OR which makes use of nodes' location information. We identify and prove three important properties of GOR. The first one is on prioritizing the forwarding candidates according to their geographic advancements to the destination. The second one is on choosing the forwarding candidates based on their advancements and link qualities in order to maximize the expected packet advancement (EPA) with different number of forwarding candidates.

In conventional opportunistic forwarding, to have a packet received by multiple candidates, either IP broadcast or an integration of routing and MAC protocol is adopted. The former is susceptible to MAC collision because of the lack of collision avoidance support for broadcast packet in current 802.11, while the latter requires complex coordination and is not easy to be implemented. In POR, we use similar scheme as the MAC multicast mode described in. The packet is transmitted as unicast (the best forwarder which makes the largest positive progress toward the destination is set as the next hop) in IP layer and multiple reception is achieved in interception.

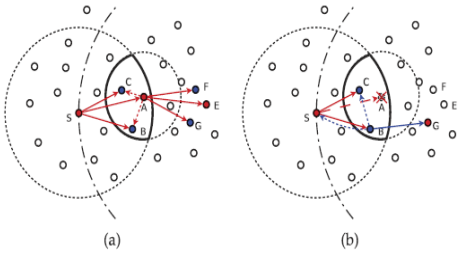

Fig. 1. (a) The operation of POR in normal situation. (b) The operation of POR when the next hop fails to receive the packet.

As the data packets are transmitted in a multicast-like form, each of them is identified with a unique tuple (src_ip, seq_no) where src_ip is the IP address of the source node and seq_no is the corresponding sequence number. Every node maintains a monotonically increasing sequence number, and an ID_Cache to record the ID (src_ip, seq_no) of the packets that have been recently received. If a packet with the same ID is received again, it will be discarded. The basic routing scenario of POR can be simply illustrated in Fig. 1. In normal situation without link break, the packet is forwarded by the next hop node (e.g., nodes A, E) and the forwarding candidates (e.g., nodes B, C; nodes F, G) will be suppressed (i.e., the same packet in the Packet List will be dropped) by the next hop node's transmission. In case node A fails to deliver the packet (e.g., node A has moved out and cannot receive the packet), node B, the forwarding candidate with the highest priority, will relay the packet and suppress the lower priority candidate's forwarding (e.g., node C) as well as node S.

3.2. Selection and Prioritization of Forwarding Candidates

One of the key problems in POR is the selection and prioritization of forwarding candidates. Only the nodes located in the forwarding area [14] would get

the chance to be backup nodes. The forwarding area is determined by the sender and the next hop node. A node located in the forwarding area satisfies the following two conditions: 1) it makes positive progress toward the destination; and 2) its distance to the next hop node should not exceed half of the transmission range of a wireless node (i.e., R/2) so that ideally all the forwarding candidates can hear from one another. In Fig. 1, the area enclosed by the bold curve is defined as the forwarding area. The nodes in this area, besides node A (i.e., nodes B, C), are potential candidates. According to the required number of backup nodes, some (maybe all) of them will be selected as forwarding candidates. The priority of a forwarding candidate is decided by its distance to the destination. The nearer it is to the destination, the higher priority it will get. When a node sends or forwards a packet, it selects the next hop forwarder as well as the forwarding candidates among its neighbors. The next hop and the candidate list comprise the forwarder list. Algorithm 1 shows the procedure to select and prioritize the forwarder list. The candidate list will be attached to the packet header and updated hop by hop. Only the nodes specified in the candidate list will act as forwarding candidates.

Algorithm 1. Candidate Selection
ListN : Neighbor List
ListC : Candidate List, initialized as an empty list
N_D : Destination Node
base : Distance between current node and N_D
if find(ListN,N_D) **then**
next_hop<-ND
return
end if
for i<- 0 to length(ListN) **do**
ListN[i]. dist<- dist (ListN[i], N_D)
end for
ListN.sort()
next hop<- ListN[0]
for i <-1 to length(List N) **do**
if dist(ListN[i],N_D)>= base or length(List C)=N
then
break
else if dist(listN[i], listN[0]) < R/2 **then**
ListC.add(ListN[i])
end if
end for

3.3. Security Implementation

Encryption is the process of converting plain text "unhidden" to a cryptic text "hidden" to secure it against data thieves. This process has another part where cryptic text needs to be decrypted on the other end to be understood. Fig.1 shows the simple flow of commonly used encryption algorithms.

In cryptography, **RC4** (also known as **ARC4** or **ARCFOUR** meaning Alleged RC4, see below) is the most widely used **Symmetric (Private key) stream cipher** and is used in popular protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic) and WEP (to secure wireless networks). RC4 generates a pseudorandom stream of bits (a keystream). As with any stream cipher, these can be used for encryption by combining it with the plaintext using bit-wise exclusive-or; decryption is performed the same way . To generate the keystream, the cipher makes use of a secret internal state which consists of two parts:1.A permutation of all 256 possible bytes (denoted "S" below).2.Two 8-bit index-pointers (denoted "i" and "j").

3.4. RC4 Algorithm

RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the ciphertext. The algorithm can be broken into two stages: initialization, and operation. In the initialization stage the 256-bit state table, S is populated, using the key, K as a seed.
The initialization process can be summarized by the pseudo-code:
j = 0;
for i = 0 to 255:
S[i] = i;
for i = 0 to 255:

j = (j + S[i] + K[i]) mod 256;
swap S[i] and S[j];

It is important to notice here the swapping of the locations of the numbers 0 to 255 (each of which occurs only once) in the state table. The values of the state table are provided. Once the initialization process is completed, the operation process may be summarized as shown by the pseudo code below;

```
i = j = 0; 50
for (k = 0 to N-1) {
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
swap S[i] and S[j];
pr = S[ (S[i] + S[j]) mod 256]
output M[k] XOR pr
}
```

Where M[0..N-1] is the input message consisting of N bits.

This algorithm produces a stream of pseudo-random values. The input stream is XORed
with these values, bit by bit. The encryption and decryption process is the same as the data
stream is simply XORed with the generated key sequence

4. Performance Evaluation

The following metrics are used for performance comparison: . Packet delivery ratio. The ratio of the number of data packets received at the destination(s) to the number of data packets sent by the source(s). The average and the median end-toend delay are evaluated, together with the cumulative distribution function of the delay. The average end-to-end path length (number of hops) for successful packet delivery. Packet forwarding times per hop (FTH). The average number of times a packet is being forwarded from the perspective of routing layer to deliver a data packet over each hop. . Packet forwarding times per packet (FTP). The average number of times a packet is being forwarded from the perspective of routing layer to deliver a data packet from the source to the destination. Among the metrics, FTH and FTP are designed to evaluate the amount of duplicate forwarding. For unicast style routing protocols, packet reroute caused by path break accounts for FTH being greater than 1. On the other hand, for those packets who fail to be delivered to the destination(s), the efforts that have already been made in forwarding the packets are still
considered in the calculation of FTH, as FTH is calculated as follows:

$$FTH = \frac{N_s + N_f}{\sum_{i=1}^{N_r} N_{hi}},$$

where Ns, Nf , and Nr are the number of packets sent at the source(s), forwarded at intermediate nodes, and received at the destination(s), respectively. Nhi is the number of hops for the ith packet that is successfully delivered. Unlike FTH, FTP averages the total number of times a packet is being forwarded on a per-packet basis:

$$FTP = \frac{N_s + N_f}{N_r}.$$

4.1. Forwarding Candidate Number Evaluation

We first evaluate the effect of the number of forwarding candidates (i.e., N) on POR's performance. Generally, larger value of N will result in higher robustness as more nodes serve as backups. In addition, the increase in the number of forwarding candidates will also enlarge the packet header, thus introducing more overhead.

4.2. Implementation Of Rc4

4.2.1. Private Key Encryption

In private key encryption technology, both the sender and receiver have the same key and use it to encrypt and decrypt all messages.

4.2.2. Stream Cipher

Stream cipher is one of the simplest methods of encrypting data where each bit of the data is sequentially encrypted using one bit of the key as shown in Fig.3.

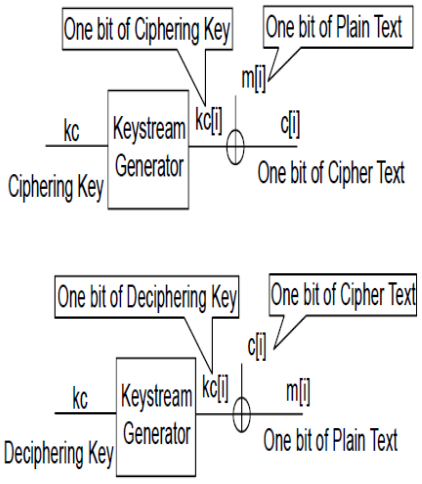

Fig.3 Stream ciphering and deciphering

In order to make a stream cipher more difficult to crack, one could use a crypto key which varies in length. This would help to mask any discernible patterns in the resulting ciphertext. In fact, by randomly changing the crypto key used on each bit of data, one can produce ciphertext that is mathematically impossible to crack. This is because using different random keys would not generate any repeating patterns which can give a cracker the clues required to break the crypto key. The main advantage of the stream cipher is that it is faster and more suitable for streaming application but its main disadvantage is that it is not suitable in some architecture. One example of the stream cipher method is the RC4 technique.

4.3. RC4 Steps

The steps for RC4 encryption algorithm is as follows:
1- Get the data to be encrypted and the selected key.
2- Create two string arrays.
3- Initiate one array with numbers from 0 to 255.
4- Fill the other array with the selected key.
5- Randomize the first array depending on the array of the key.
6- Randomize the first array within itself to generate the final key stream.
7- XOR the final key stream with the data to be encrypted to give cipher text.

5. Conclusion

In this paper, we propose for a secured data transmission between the source and destination in a vulnerable network. The mobile ad hoc network is constantly changing resulting in dynamic mobile network, where destination location varies at each time. In the face of frequent link break due to node mobility, substantial data packets would either get lost, or experience long latency before restoration of connectivity. Thus we proposed Position based Opportunistic Routing (POR) Protocol that is not susceptible to node mobility and duplicate relaying. Also to increase the security of data, it is encrypted using RC4 algorithm. The data packet is sent in a cipher text format to the destination where it is decrypted to obtain the original data.

The problem of communication void also exists. During communication holes, the Position based Opportunistic Routing protocol cannot be used. Thus a Virtual Destination-based Void Handling scheme is implemented to overcome the cons of communication voids. Also, the RC4 encryption algorithm is a symmetric (private key) stream cipher and is vulnerable to analytic attacks and also susceptible to generate weak keys. Thus to enhance the level of security, stronger encryption algorithm which uses public key can be implemented.

References

[1].J.Broch,D.A.Maltz,D.B.Johnson,Y.C.HU,and J.Jetcheva,"A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," Proc.ACM MobiCom,PP.85-97,1998.

[2]. B.Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," Proc.ACM MobiCompp.243-254,2000.

[3]. E.Rozner,J.Seshadri,Y.Mehta an L.Qiu, "SOAR:Simple Opportunistic Adaptive Routing Protocol for Wireless Mesh pp.1622-1635,Dec.2009

[4]. D.Cen,J.Deng and P.Varshney, "Selection of a Forwarding Area for Contention-Based Geographic Forwarding in wireless Multi-Hop Networks," IEEE Trrans. Mobile Computing,vol.8,no.5,pp.31111-3122,sept.2007.

[5].N.Arad and Y.Shavitt, "Minimizing Recovery State in Geographic Ad Hoc Routing,"IEEE Trans. Mobile Computing, Vol.8, No.2, pp. 203-217, Feb 2009.

[6] S. Biswas and R. Morris, "EXOR: Opportunistic Multi-Hop Routing for Wireless Networks," Proc. ACM SIGCOMM, pp. 133-144, 2005.

[7] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading Structure for Randomness in Wireless Opportunistic Routing," Proc. ACM SIGCOMM, pp. 169-180, 2007.

[8] E. Rozner, J. Seshadri, Y. Mehta, and L. Qiu, "SOAR: Simple Opportunistic Adaptive Routing Protocol for Wireless Mesh Networks," IEEE Trans. Mobile Computing, vol. 8, no. 12, pp. 1622-1635, Dec. 2009.

[9] A. Balasubramanian, R. Mahajan, A. Venkataramani, B.N. Levine, and J. Zahorjan, "Interactive WiFi Connectivity for Moving Vehicles," Proc. ACM SIGCOMM, pp. 427-438, 2008.

[10] K. Zeng, Z. Yang, and W. Lou, "Location-Aided Opportunistic Forwarding in Multirate and Multihop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 6, pp. 3032-3040, July 2009.