Secure End-to-End Data Transmission using Data Obfuscation Method for Multipath Routing Protocol

Nimitr Suanmali
Suan Dusit Rajabhat University
295 Rajasima rd. Dusit Bangkok
nimitrs@hotmail.com

Kamalrulnizam Abu Bakar
Department of Computer System and Communication
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia
kamarul@fsksm.utm.my

ABSTRACT
Multipath routing is the routing technique of leveraging multipath through a network, which can yield a variety of benefits such as fault tolerance or increased bandwidth. In Mobile Ad Hoc Network (MANET), the specific characteristic of this network make cooperation among all nodes in the network. The transmission range of each node is limited. Thus, each node needs to perform routing, data delivery, forward control packets for others. An ad hoc network can work effectively only if the participating nodes cooperate in a proper way. These characteristics make secure data transmission more important. In our paper title, Secure End-to-End Data Transmission using Data Obfuscation Method for Multipath Routing Protocol, will focus on the security of end-to-end data transmission using data obfuscation method for multipath routing protocol. The previous research proposed several ideas to secure data transmission, but rely on complicated encryption and trusted third party. We will use the advantage of data obfuscation method to make our scheme more secure.

Categories and Subject Descriptors
A.1[General Literature]: Introductory And Survey

General Terms
Security

Keywords
Data Obfuscation, Data Security, MANET, Multipath Routing

1. INTRODUCTION
One of the most important characteristics of Ad Hoc networks is that they require no centralized administration or fixed network infrastructure[1]. Nodes in the ad hoc networks cooperate with each other to do routing discoveries and data transmissions in a self-organized way. Self-organization is the nature of ad hoc networks. It will beat others when used in the applications without existing infrastructure or any other trusted authorities. However, it is this self-organization nature that makes mobile ad hoc networks insecure. Without any third-party authority, everybody including some malicious nodes can join and leave the ad hoc network freely. These malicious nodes would then perform all kinds of attacks to eavesdrop information, interrupt normal communications, or even make the whole network denial-of-service[2].

Several security schemes for mobile ad hoc networks have been proposed in order to protect the routing information or data packages during communications[3-8]. However, most of these schemes assume that there are trusted third parties or centralized servers who are responsible for issuing certain certificates and keys or monitoring the behaviors of other nodes. Centralized servers or trusted parties make the network more controllable but they destroy the self-organizing nature and reduce the scalability of mobile ad hoc networks. Even some schemes distribute the servers into many nodes, there are still bottlenecks due to centralization. If one scheme distributes the functions of servers into each node of the network, it will introduce huge performance overhead.

Secure data delivery from one node to another is a fundamental service in a mobile ad hoc network as well as in any network. Sensitive information transmitted across a hostile mobile ad hoc network should be protected from passive attacks, such as eavesdropping. The wireless channel in a hostile environment is vulnerable particularly to eavesdropping due to its broadcast nature. Conventionally, data confidentiality is achieved by cryptography. However, the security of cryptographic methods highly depends on the secure and reliable key management system[9]. Many computationally efficient cryptographic algorithms, such as the stream cipher RC4 [10] which is suitable in the resource constrained device, are highly sensitive to the keying materials and susceptible to the known plaintext attacks. Many efforts have been made in developing more secure and more reliable key management systems [11-14]. However, in a highly dynamic mobile ad hoc network environment, end-to-end encryption is usually impractical.

From the problem statement above, it is needed to secure the data communication in mobile ad hoc network due to various sensitive applications. The focus of this scheme is to secure the data communication part of mobile ad hoc network.

The remaining of this paper is organized as follow. In section 2, described about the existing type of secure end-to-end data transmission. In section 3, provide a brief summary of the security aspects of the existing secure data transmission scheme. In section 4, describe the architecture design of our secure end-to-end data transmission scheme. Finally, we conclude and point out the future work.

688
2. EXISTING TYPE OF SECURE END-TO-END DATA TRANSMISSION

In this section, we describe the existing of secure end-to-end data transmission schemes.

2.1 A Multipath Routing Approach for Secure Data Delivery

A multipath routing approach for secure data delivery [15] is a novel approach to enhance data confidentiality when transmitting across the insecure networks. This protocol combined the secret sharing scheme and the advantage of multipath routing to enhance data confidentiality when transmitting across the insecure network. The idea is to take advantage of the distributed nature of networks such as Internet or wireless networks and combine the secret sharing scheme and multipath routing. With a (T,N) secret sharing scheme, the secure message is divided into N shares such that from any T or more shares, they can easily recover the message, while from any T-1 or less shares, it is computationally impossible to recover the message. Then using multipath routing algorithm, the shares are delivered across the network via N different paths, where no T or more paths can share a single node. The destination node reconstructs the original message upon receiving T or more shares.

2.2 Data Security in Ad hoc Network using Multipath Routing

Data Security in Ad hoc Network using Multipath Routing is a solution for securing data in Ad hoc network[16]. This protocol exploited the existence of multiple paths between nodes in an Ad hoc network to increase the robustness of transmitted data confidentiality. In ad hoc network, security depends on several parameters and reaching a good security degree is a hard task. This protocol started by taking into consideration network topology. It used n routes (n>=3) among N available route existing between the sender and the receiver. It used two types of channel, signaling channel and carries user data channel. Then, the protocol divided the message into (n-1) parts that each of them has a unique identifier. It generated a random integer number to be sent on one path then encrypted message parts using WEP encryption. The author added a layer on top of transport layer (TCP/UDP), so this algorithm can be run with both reactive and proactive routing protocol.

2.3 Secure Data Transmission in Mobile Ad Hoc Network

Secure Message Transmission (SMT) is a secure multipath routing protocol which safeguards the data transmission against arbitrary malicious behavior of other nodes[17]. This is a lightweight protocol that can operate solely in an end-to-end manner. The protocol divided a message into (n-1) parts that each of them has a unique identifier. It exploits the redundancy of multi-path routing and adapts its operation to remain efficient and effective even in highly adverse environments. The SMT protocol safeguarded pair-wise communication across an unknown frequently changing network, possibly in the presence of adversaries that may exhibit arbitrary behavior. It combined four elements: end-to-end secure and robust feedback mechanism, dispersion of the transmitted data, simultaneous usage of multiple paths, and adaptation to the network changing conditions. SMT detected and tolerated compromised transmissions, while adapting its operation to provide secure data forwarding with low delays. After the source invoked the route discovery protocol and initiated the Active Path Set (APS), it dispersed each outgoing message into a number of pieces. Each dispersed piece is transmitted across a different route and carries a Message Authentication Code (MAC)[18], so that the destination can verify its integrity and the authenticity of its origin. The goal of SMT is to ensure secure data forwarding, after the discovery of routes between the source and the destination has been already performed.

2.4 Multipath Routing Based Secure Data Transmission

Multipath routing based secure data transmission is a secure multipath routing scheme[8] which combined with feedback mechanism to tackle misbehaviors on data delivery formed by one or more misbehaving node in ad hoc network. Data and control packet are transmitted through two node-disjoint paths. The source is notified of suspected misconduct of intermediate nodes through feedback mechanism. As the scheme builds an end-to-end feedback channel from the destination to source, any misbehavior causing a certain number of data packets losing during the proceed of transmission can be informed to the source. The author claimed that in a network with up to 40% misbehaving nodes, the proposed scheme and the derivation result in around 17% in data receive rate over the single path DSR.

2.5 Secure Protocol for Reliable Data Delivery (SPREAD)

Secure Protocol for Reliable Data Delivery (SPREAD) is a secure multipath routing scheme to enhance security of end-to-end data delivery in a mobile ad hoc network[19]. The basic idea of SPREAD is to transform a secret message in to multiple shares and then deliver the shares via multiple paths to the destination. The fundamental idea of SPREAD is based on two techniques, multipath routing and secret sharing. Each message has a security level and the availability of multiple path. The message was divided into multiple pieces by the used of (T,N) threshold secret sharing algorithm and sends them through multiple path. When a source node wants to send a message to a destination node securely in a MANET, the source can use a multipath routing algorithm to find multiple paths from the source to the destination with certain properties (e.g., disjoint paths); then the source determines a secret sharing scheme, depending on the message security level and the availability of multiple paths, to transform the message into multiple shares; then the message shares are routed to the destination by the multipath routing protocol and the destination reconstruct the original message upon receiving a certain number of shares.
2.6 Secure Multipath Scheme for Mobile Ad Hoc Network

Secure Multipath Scheme for Mobile Ad Hoc Network is a secure framework for multipath mobile ad hoc networks that provides end-to-end security between the source-destination pair[20]. The main goal of this framework is to provide security not only on the multipath ad hoc routing protocol but also on data transmission using these multiple routes. This proposed framework is designed on based of source routing such as DSR. They assumed that a source node (S) and a destination node (D) share some secret information between them. For the key distribution, they considered self-certified public keying technique [21, 22], so any node in the network can compute another node's public key knowing public parameter, ID and CA's public key. The route from source S to destination D will be obtained by flooding of RREQ. When a node received an RREQ packet with source address S and destination address D, it looked at its Intermediate node table. Intermediate node table maintained the list of recent most RREQ received for any source destination pair and the intermediate nodes for the request. If the packet arrived has a list of intermediate nodes that is a superset of what is there in the routing table, the packet is discarded else the node adds its own entry into the packet and rebroadcasts it. In data forwarding, session keys SKS and SKD are used to encrypt and hash packets transmitted respectively. Apart from doing encryption and hashing, the packets would be divided in \( n \) fragments that would be sent to the destination on \( n \) different routes.

3. DISCUSSION

Table 1 provides a brief summary of the security aspects of the secure data transmission scheme above. Each scheme has different security method, but some schemes have same security method. Multipath Routing Approach for Secure Data Delivery scheme and Reliable Protocol for Reliable Data Delivery used same security method, (T,N) secret sharing. The (T,N) secret sharing avoided complex encryption by divide deliver message into \( N \) shares and send to destination through multiple path. Even though (T,N) secret sharing can be enhanced security of deliver message, it produced huge overhead. Data Security in Ad Hoc Network using Multipath Routing used WEP encryption to increase the robustness of transmitted data confidentiality, but it was attacked by Chop Chop Attack[23]. Multipath Routing based Secure Data Transmission scheme used feedback mechanism to safeguard the data transmission. Eventhough the feedback mechanism can be informed status of data packet to the source node in real time manner, it consumed 1 communication channel for this mechanism. Secure Message Transmission scheme used Message Authentication Code (MAC) to safeguard the data transmission. The strength of MAC was easily breakdown by short time calculation[24]. Thus, we will consider another security aspect, such as data obfuscation, to improve the confidentiality of transmitted data in mobile ad hoc network.

<table>
<thead>
<tr>
<th>Protocol/Scheme</th>
<th>Approach</th>
<th>Security Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Multipath Routing Approach for Secure Data Delivery(2001)</td>
<td>-To enhance data confidentiality</td>
<td>- (T,N) secret sharing</td>
</tr>
<tr>
<td>Data Security in Ad Hoc Network using Multipath Routing(2003)</td>
<td>-To increase the robustness of transmitted data confidentiality</td>
<td>- WEP Encryption</td>
</tr>
<tr>
<td>Secure Message Transmission (SMT)(2003)</td>
<td>-To safeguard the data transmission</td>
<td>- Message Authentication Code (MAC)</td>
</tr>
<tr>
<td>Multipath Routing based Secure Data Transmission(2006)</td>
<td>-To secure data and control packet</td>
<td>- Feedback Mechanism</td>
</tr>
<tr>
<td>Secure Protocol for Reliable Data Delivery (SPREAD)(2007)</td>
<td>-To enhance security of end-to-end data delivery</td>
<td>-(T,N) secret sharing</td>
</tr>
<tr>
<td>Secure Multipath Scheme for Mobile Ad Hoc Network(2008)</td>
<td>-To enhance end-to-end security</td>
<td>-Self-certified Public Key</td>
</tr>
</tbody>
</table>

4. METHODOLOGY

This section will describe the architecture design of the secure end-to-end data transmission scheme. This scheme consists of two main processes, initialization process and data transmission process. The details of both processes are described as follow.

4.1 Initialization Process

We assume that all participant nodes are located in the same network domain, called “Obfuscation Environment”. With this assumption, the Obfuscation Environment starts by a starter node, called “Initiator”. To start the Obfuscation Environment, the initiator authenticates participant nodes with authentication technique such as self-certified public keying technique [21, 22]. The initiator defines system parameters and generates a secure key that will be used in data obfuscation module during the secure data transmission process. The participant nodes prepare an identity information such as user name, IP address or other personal related information and then send these information to the initiator for secure key generation. Figure 1 illustrates the initialization process of Obfuscation Environment.
After finish authentication, the initiator node will distribute a secret key to all participant nodes for using as an obfuscation key. To strengthen the secret key, the initiator will update the secret key periodically. Finally, authenticated nodes perform Obfuscation Environment to establish data transmission.

4.2 Secure Data Transmission Process
This proposed scheme consists of 5 modules, splitting module, obfuscation module, key sharing module, deobfuscation module and merging module. The details of each module are shortly described below. Figure 2 shows the general structure of the proposed scheme.

Splitting Module
The original message will split into small group. The message is a string of characters consist of b₁,b₂,b₃,…,bₙ. The characters bₙ are eight-bit integers taken from a certain range [0-255]. Then, the split data will put into MxN matrix.

Obfuscation Module
In the obfuscation module, it can be separated into two process, data obfuscation and route obfuscation. For data obfuscation, the message from splitting module will put into MxN matrix, order by column. After that, the obfuscation module will mess up data in the matrix using obfuscation method such as data swapping method using XOR algorithm. The XOR algorithm is used to combine the key and the actual data to make it difficult to understand. The key k is a binary number which is random by the obfuscation module. Let b is a one byte binary data. To obtain the obfuscated data o, the function to generate the obfuscated data is:

\[ o = \text{XOR}(b, k) \]

The obfuscation module not only obfuscated the actual data, but also obfuscated the route number of each splitting data piece. For route obfuscation, the row number of each matrix refers to the route number. The XOR algorithm is used to combine the key and row number of matrix to make the route number more difficult to guess.

Obfuscation Key Sharing Module
In obfuscation key sharing module, the key used in obfuscation module will be sent to destination by adding a flag of secret key in data packet. To strengthen the data confidentiality, the secret key will be used randomly for each data piece. The secret key provided to all participant nodes by the initiator at the initialization process.

Deobfuscation Module
This module happened at the destination side. After the obfuscated data reached the destination, the destination will deobfuscate the received data using the obfuscation key which is sent from the source. The destination arranged the received data into MxN matrix. After that, the received data will be deobfuscated, one by one order by column, using the key which send from the source.

Merging Module
The last process of the proposed scheme is merging module. After finished deobfuscation module, the merging module read data from the matrix, order by column, to reconstruct the message.

5. CONCLUSIONS
This paper has described a method and framework of secure data transmission scheme based on multipath routing using data obfuscation method to improve the security of end-to-end data transmission. In this paper, the data was splitting into small pieces by splitting module and obfuscated by obfuscation at the source node. Then, the data was transmitted to the destination through multipath routing protocol. The implementation of obfuscation method is not only happened on data transmission, but also on key sharing process and route selection. Finally, the data was reconstructed at the destination side by deobfuscation module and merging module. The goal of this paper is to find the appropriate method to secure the data transmission on multipath routing protocol in MANET which is vulnerable to attack from inside and outside attacker. In order to achieve the objectives,
secure end-to-end data transmission scheme that utilizes the advantage of data obfuscation method has been proposed.

6. REFERENCES