ISSN:2321-1156
International Journal of Innovative Research in Technology & Science(IJIRTS)

REDUCING DATA COMPROMISATION BY MULTIPATH ROUTING IN MANET

Gaurav Tidke, Student, Department of Computer Technology,
Yeshwantrao Chavan College of Engineering, Nagpur, India
Mohit Keshwani, Student, Department of Computer Technology,
Yeshwantrao Chavan College of Engineering, Nagpur, India
Pratik Barachha, Student, Department of Computer Technology,
Yeshwantrao Chavan College of Engineering, Nagpur, India
Harshal Wankhade, Student, Department of Computer Technology,
Yeshwantrao Chavan College of Engineering, Nagpur, India
Mrs.Smita Kapse, Assist Prof, Department of Computer Technology,
Yeshwantrao Chavan College of Engineering, Nagpur, India

Abstract

We modified the existing technique of sending data from sender to recipient. We used threshold secret sharing algorithm in conjunction with the multipath routing algorithm. The idea is to convert the message to be sent into multiple shares using threshold secret sharing scheme at first. Then delivering these shares to the recipient via different available paths using multipath routing algorithm. System is designed in such a way that the interceptor cannot understand anything about whole message even if he is able to intercept some message shares. Thereby achieving security as well as reliability in data transfer form sender to recipient in MANET environment.

Keywords

MANET, Threshold Secret Sharing, Multipath Routing, NS2, maximal node disjoint path finding algorithm, Lagrange's interpolation formula.

Introduction

Mobile ad hoc networks' (MANETs) rapid deploy ability and self-organizing configurability have made them very attractive in tactical and military applications, such as the tactical communications in a battlefield, where the environment is hostile and fixed infrastructures are not available or reliable, but fast network establishment, self-reconfiguration and security-sensitive operations are necessary. On the other hand, the salient features of a MANET, such as the broadcast nature of the wireless channel, the infrastructure less architecture, the highly dynamic network topology, and the limited resources of mobile devices, have posed many new challenges in the design and implementation of such a network [1].

Secure data delivery from one node to another is a fundamental service in a MANET as well as in any network. Sensitive information, such as tactical military information, transmitted across a hostile MANET 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.

Related Work

The combination of secret sharing and multipath routing was first proposed by Zhou and Haas in [2] where the role of a certificate authority in a public key infrastructure is distributed to multiple servers by the means of secret sharing and multipath routing. This idea was further developed by Kong et al. in [3] where CAs are further localized by distributing the servers more evenly in the network such that operations such as signing a certificate can be done locally by neighbors of the requesting node. A more recent key management approach based on multipath routing is a probabilistic approach for the establishing of pairwise secret keys [6]. The multipath in their schemes are logical (i.e., encrypted by different keys) rather than physically independent (node-disjoint) paths required in our secret sharing scheme.
Reducing data compromise by multipath routing

A. Introduction

The fundamental idea comes from the following observation: a messenger who carries the full message from one place to another place across a hostile ground may reveal the message easily if he/she is captured, while the message will not be fully recovered by adversaries if multiple messengers are deployed, each only carrying partial information and taking different routes across the hostile ground.

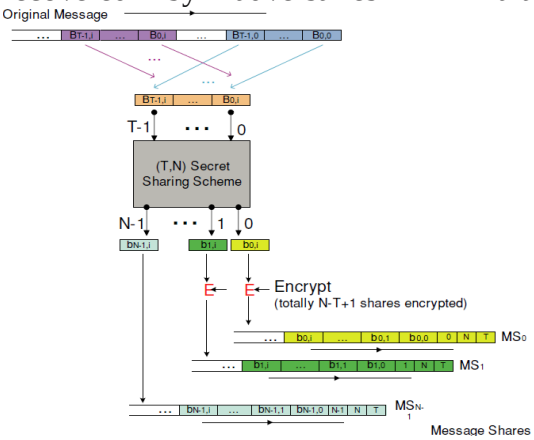

Figure. (T, N) Secret sharing system

B. Threshold Secret Sharing:

The first issue is how to divide the message into multiple pieces (shares)? In this technique, we use the threshold secret sharing algorithm to divide the message into multiple pieces. With a (*T*, *N*) secret sharing algorithm [5], the secret message can be divided into *N* pieces (called *message shares*) such that in order to compromise the message, the adversary must compromise at least *T* shares. With fewer than *T* shares, the enemy cannot learn anything about the message and has no better chance to recover the secret than an outsider who knows nothing at all about the message achieving desirable security.

According to the secret sharing algorithm, the probability that the message is compromised equals the probability that *T* or more shares are compromised. We denote the probability that the message is compromised in terms of the share allocation *n* as *Pmsg*(*n*). Then, the share allocation can be formulated using Lagrange's Interpolation formula [6]:

$$f(x) = \sum_{i=1}^{t} yi \prod_{1 \le j \le t} \frac{x - xj}{xi - xj}.$$

C. Multipath Routing

The issue is how to allocate the shares onto each selected path so that the adversary has least possibility to compromise the message. The simplest and most intuitive share allocation scheme is to choose *N* as the number of available paths, apply (*T*, *N*) secret sharing, and allocate one share onto each path. However, in an ad hoc network, wireless links are instable and the topology changes frequently.

Packets might be dropped during the transmission. For this issue, it is usually necessary to introduce some redundancy (i.e., $T<N$) in the scheme to improve the reliability, i.e., the destination would have better chance to receive enough shares for reconstructing the message. The third issue is the multipath routing [6].

Maximal node disjoint paths finding algorithm [6]:

Step 1. Find the first most secure path by modified Dijkstra algorithm [6], select the path

Step 2. Perform a graph transformation as follows-

For each selected path:

(a) Replace the links used in the path with directed arcs – for the arc that is directed towards the source, make its cost the negative of the original link cost; make the cost of the arc directed towards the destination infinite (i.e., remove it)

(b) Split each node on the selected paths (except the source and destination) into two co-located sub nodes; Connect the two sub nodes by an arc of cost 0 and directed towards the source node.

(c) Replace each external link that is connected to a node in the selected paths by its two component arcs of cost equal to the link cost – let one arc terminate on one sub node and the other one emanate from the other sub node such that along with the zero-cost arc, a cycle does not result.

Step 3. Run the modified Dijkstra algorithm, find the most secure path in the transformed graph

Step 4. Transform back to the original graph; erase any interlacing edges; group the remaining edges to form the new path set.

Step 5. Go to step 2, until no more path can be found or the security of the path set does not increase.

Conclusion

In this paper, the basic idea is to distribute the secret, first by secret sharing algorithm at the source node to generate message shares and then by multipath routing to deliver message shares across the network, so that in the event that a small number of shares are compromised, the secret message as a whole will not be compromised. We also show that a redundant scheme can be designed in such a way that a certain degree of reliability can be provided without sacrificing the security. Therefore, idea is a suitable and promising approach to improve network security in the highly dynamic MANET environment.

References

[1] W. Lou and Y. Fang, A multipath routing approach for secure data delivery, in: *IEEE Military Communications Conference (MILCOM 2001)* (Mclean, VA, USA, Oct. 2001).

[2] L. Zhou and Z.J. Haas, Securing ad hoc networks, IEEE Network magazine 13(6) (November/December 1999).

[3] J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, Providing robust and ubiquitous security support for Manet, in: *ICNP* (2001)

[4] W. Lou, W. Liu and Y. Fang, SPREAD: Improving network security by multipath routing, in: I*EEE Military Communications Conference (MILCOM 2003)* (Boston, M, and Oct. 2003).

[5] W. Lou, W. Liu and Y. Fang, SPREAD: Enhancing data confidentiality in mobile ad hoc networks, in: *IEEE INFOCOM 2004* (Hong Kong, China, Mar 2004)...

[6] L.Eschenauer and V. Gligor, A key-management scheme for distributed sensor networks, in: ACM CCS 2002 (Washington, DC, 2002).
[6] A. Shamir, How to Share a Secret, Communications of the ACM 22(11) (Nov 1979) 612–613.