MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

Dear Authors : **Seyed amir hoseini, Mahdi hoseinzade** and **Mahdi javanmard**

We are delighted to inform that your research paper has been **"Accepted for Publication"** in Life Science Journal with minor revision.

Paper Title: *A Novel Hybrid Method for Efficient Key Distribution with sponsorization in Mobile Ad hoc Networks*

We really hope if you can help to improve our journal by citing it's articles in other journals! You can simply use the message in the end of the article abstract to cite it. Please consult the following website for the template associated with the journal to which you wish to submit your article(template also attached):

http://www.sciencepub.net/marslandfile/template

Please read your manuscript again and send me your revised/formatted version following the attached template. For your revised file please follow the attached template. It must be a single doc version file saved by the file name containing file number (pay attention to the page setup, end of abstract, font, etc)! Even if your submitted manuscript is the final version following the required format, you still need to send it to me again by the file name containing file number! If this manuscript has been sent to us and has a file number before, please note me it.

Thanks!

Ma, Hongbao, PhD
Marsland Press
PO Box ١٨٠٤٣٢, Richmond Hill, New York ١١٤١٨, USA
http://www.sciencepub.net; sciencepub٧@gmail.com;

We hope that you can help to improve the journals of Marsland Press, such as to cite and link our papers, promote our journals/papers/websites in Internet (e.g. Medline, EBSCO, Google, Facebook, Twitter, Wikipedia, Linkedin, blog), and make them indexed by academic databases, etc. You can simply use the message in end of the article abstract to cite it.

As the size of our email account sciencepub٦@gmail.com is full, we have forwarded it to sciencepub٧@gmail.com. Please note that sciencepub٧@gmail.com is same as sciencepub٦@gmail.com

Hybrid Method for Key Distribution in Mobile Ad hoc Networks

Abstract

There is a need for security services to provide group-oriented communication privacy and data integrity. It is important that members of the group can establish a common secret key for encrypting group communication. A secure distributed group key agreement and authentication protocol is required to handle this issue. Early, key tree approaches have been proposed to distribute group key in such a way that the rekeying cost scales with the logarithm of the group size for a join or leave request. The effciency of this key tree approach critically depends on whether the key tree remains balanced over time as members join or leave. Instead of performing individual re-keying operations, an interval-based approach of re-keying is adopted in the proposed scheme. In other hand, Self-healing group key distribution is essential aimed to achieve efficient key distribution in Mobile Ad hoc Networks over lossy and dynamic communication channels. In particular, we propose the concept of hierarchical self-healing group key distribution with interval time rekeying process. Indeed, we develop an efficient hybrid method based on three important concepts: Hierachicaly, self-healing and time interval rekying. Simulation results show dramatic improvement in network parameters e.g., end to end delay, packet delivery ratio.

Introduction

Due to mobility of nodes, traditional security models designed for fixed-network topologies may not be fully applicable in infrastructureless wireless networks. each efficient and secure key distribution scheme, the designers should consider many factors such as application requirements, network topologies, and packet loss characteristics of the underlying wireless networks. Generally speaking, security in wireless networks has six challenges [٩،١٠]: Lack of fixed infrastructure, Resource limitations on wireless devices, Unknown network topology, Wireless nature of communications, Very large density of distribution of wireless nodes and High risk of physical attacks to unattended nodes. Cryptographic techniques in network security can be applied to ad hoc networks [١] . Key management is the main component in security. If the key size is large, the corresponding cryptographic algorithm ensures a guaranteed secure communication, but lead to more energy consumption. Hence energy efficient key management techniques are used in wireless networks. Secure and efficient key management in ad hoc networks [٢] builds a public key based on shared secret key and node servers. Each server creates its Certificate Authority (CA) within a time period and updates node request based on ticket based approach. During key update the compromised node is recognized and key certificate is revoked. Scalable Key management and clustering [٣] is based on hierarchical network partitioning and resilient to node mobility. Hierarchical Key Management [٤] for secure group communication encrypts the packet twice due to frequent changes in network topology. Source node generates private key, encrypts the data packet and forwards it to immediate node at next level one (level ١). The intermediate nodes further encrypt the data packet again and forwards it to next level (level ٢) process is repeated to level two. Distributed key management based on key update performs better compared to request update schemes. Distributed symmetric key management [٥] considers pre-key distribution and overcomes the limitation of Trusted Third Parties (TTP) key schemes. [٦] Explains the secure key management for MANETs. Light weight group key management is used to minimize the load of security protocols Distributed Lightweight group-key management [٧] based on secure optimized link state routing, use group keys for authentication control and save the node energy. The group keys are managed based on network partitions and node sessions (join/leave the route paths). Unauthorized nodes are restricted by using periodic and event based group-key replacement. Scalable cryptographic key management [٨] based on public key cryptography solves sybil attack and dynamic node deployment.