Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X

Vol.3 Issue 4 (2017) 104 - 108. Submitted 06/11/2017. Published 17/12/2017

SECURE OVERLAY ROUTING USING KEY PRE-DISTRIBUTION A LINEAR DISTANCE OPTIMIZATION APPROACH

[1]M. Kalaiyarasi, M.Phil Scholar, Bharathiyar Arts And Science College For Women, Deviyakurichi, Thalaivasal, Salem.

[2]R. Vasugi, Asst. Professor, Bharathiyar Arts And Science College For Women, Deviyakurichi, Thalaivasal, Salem.

Abstract:

An important pool for key pre-distribution schemes that's built based on symmetric cryptography concepts contains secret pairwise keys. In this particular paper, we reference the network layer since the underlay layer together with cryptographic layer since the overlay layer. Our recommended option is basically damaged whipped cream an LP problem derived by relaxing all of the Boolean constraints inside the original problem. The effectiveness of our formula reaches solving the Boolean LP challenge with a while complexity not exceeding individuals of solving the relaxed LP problem while guaranteeing to know the very best solution. We noted the main advantage of our formula as acquiring the opportunity to solve the very best routing problem for each graph either directed or undirected in addition to weighted or unweighted.

Keywords: LP Problem, Boolean, Crytographic.

1. INTRODUCTION

It's observed that routing using key pre-distribution schemes requires a two-layer formula able to find the underlay path following a corresponding overlay path. Secure routing techniques using key pre-distribution algorithms require special algorithms able to find optimal secure overlay pathways [1] [2]. Clearly, the content is decrypted and encrypted simply by the intermediate nodes around the overlay path and all sorts of other nodes which take part in routing just begin to see the encrypted message. The primary contribution of the paper is proposing a safe and secure routing formula jointly optimizing underlay and overlay pathways using key pre-distribution schemes although not requiring explicit trust of other network nodes. To be able to assess the performance and security strength from the suggested formula, we put it on numerous uneven and symmetric key pre-distribution schemes suggested [3]. We perceive our act as an operating alternative of secure network routing applications requiring key distribution. The primary drawback to the fundamental probabilistic key pre- distribution is when an assailant compromises several nodes, many links might be potentially made insecure. requirement for infrastructure and central servers along with the requirement for multiple routing domains at the expense of storing a small amount of per node keys and minimal additional price of file encryption-understanding. Liu and Ning propose storing bivariate polynomials rather of keys requiring neighboring nodes to possess a minimum of one common polynomial. Balanced incomplete block design is really a combinatorial design methodology utilized in key pre-distribution schemes. BIBD arranges v distinct key objects of the key pool into b different blocks each block representing a vital ring allotted to a node. Generally, deterministic key pre-distribution schemes

aren't scalable and want an extremely large space for storage. The majority of the key pre-distribution schemes pick the keys at random but there are many others that attempt for selecting keys in smarter ways. Key pre-distribution schemes are classified into deterministic and probabilistic algorithms. Both in groups, each network node is pre-packed with several keys selected from the key pool within the initialization phase.

2. RELATED WORK

Key pre-distribution formula by which each set of neighboring nodes possess a common key having a specific probability. Disadvantages of existing system: Deterministic key pre-distribution schemes aren't scalable and want an extremely large space for storage.

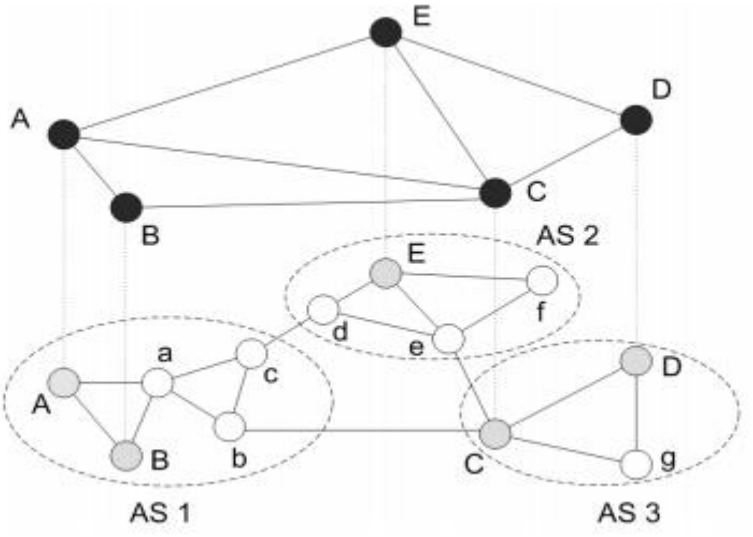

Fig.1.key Networks

The primary drawback to the fundamental probabilistic key pre-distribution is when an assailant compromises several nodes, many links might be potentially made insecure. The primary contribution of the paper is proposing a safe and secure routing formula jointly optimizing underlay and overlay pathways using key pre-distribution schemes although not requiring explicit trust of other network nodes. More particularly, the contributions of the paper are: Modeling a network using key pre-distribution schemes with directed and weighted graphs, Proposing a Boolean LP problem for optimal overlay routing within the resulting network graph, Analytically lowering the Boolean LP problem to some relaxed LP problem and therefore solving the Boolean LP in polynomial time, and Evaluating network performance, security, and consumption characteristics from the suggested formula for symmetric and uneven key pre-distribution methods operating on the top of on-demand routing protocols [6]. Benefits of suggested system: We model a network having a weighted directed graph by which all edges and vertices their very own cost. A safe and secure routing formula for that modeled graph utilizing a Boolean LP problem. Employed for secure routing in almost any network using any key pre-distribution plan. Experimental results reveal that our formula improves network performance and enhances network security.

3. PROPOSED SYSTEM

In comparison, PAKP doesn't need to send any other information in the routing packets. To be able to compensate from the faster speed of symmetric cryptography compared to uneven cryptography, we pressure each set of nodes to agree with a pairwise key for file encryption and understanding within the PAKP method. A greater quantity of intermediate understanding-file encryption steps increases the prospect of an foe node being able to access messages.

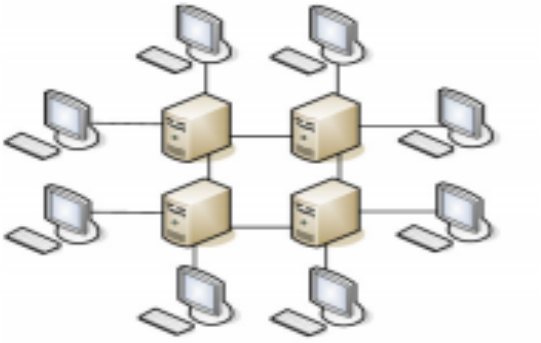

Fig.2.Architecture

Peer-to-peer networks run on top of the Internet. Peer-to-peer networks are distributed systems where the software running on each node provides equivalent functions. A definition of P2P networking is a set of technologies that enable the direct exchange of services or data between computers. Implicit in this definition are the fundamental principles that peers are equals. P2P systems emphasize sharing among these equals. A pure peer-to-peer system runs without any centralized control or hierarchical organization. A hybrid system uses some centralized or hierarchical resources. Peers can represent clients, servers, routers, or even networks Although IP multicast approaches can be considered to be solutions for various new emerging services which require active participation from many users, they do not work well in the current Internet which is based on unicast communications. authors propose to combine two mechanisms by deploying a protocol stack and design a two-layered architecture for media streaming in overlay networks. The first layer is a generic and customizable protocol which is able to construct and maintain different types of meshes. The second layer is responsible for data propagation to the nodes in the mesh by constructing an optimized diffusion tree. The goal of this modular approach is to address some inherent problems in tree-based overlay streaming solutions, in particular the vulnerability of the diffusion tree against failures and its poor resource utilization. This architecture is lightweight in terms of bandwidth usage and maintains an acceptable average reception rate. It is known that overlay routing enhances both reliability and performance of IP networks. This is because it can bypass network congestion and transient outages by forwarding traffic through one or more intermediate overlay nodes. Therefore, there are many researchers working on the design of algorithms for multicast applications in overlay networks.

4. ANALYSIS

The second algorithm is intended for group-shared applications such as videoconference, distributed games, file sharing, collaborative software and replicated database; it constructs a virtual shared tree among group members. The objective of both algorithms is to achieve traffic balancing on the overlay network so as to avoid traffic congestion and fluctuation on the underlay network, which cause low performance. To

address these problems, the algorithms actively probe the underlay network and compute virtual multicast trees by dynamically selecting the least loaded available paths on the overlay network. This way, network resources are optimally distributed and the number of multicast trees that can be setup is maximized. Both algorithms can offer service differentiation, i.e., they provide QoS guarantees at the application-layer without IP-layer support.

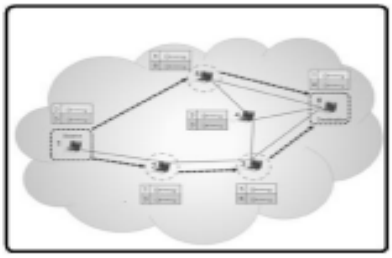

Fig.3.Framework

The low computational complexity of the proposed algorithms leads to time and resource saving. the authors consider overlay multicast in the scenarios where any participant node is a potential data source. Existing multicast algorithms for single-source always require a long time to deliver messages or have high maintenance overhead when multiple data sources are allowed. However, there are other algorithms that are designed for multi-source scenarios, but they consume too much network resources and have a long convergence time because of proximity ignorance. They propose an algorithm called FPCast, which leverages node heterogeneity and proximity information at the same time. Physically close nodes are grouped into clusters and each cluster selects a powerful, stable node as its rendezvous point. The rendezvous nodes form a DHT-based structure. Massive content distribution on overlay networks stresses both the server and the network resources because of large volumes of data to be transmitted, relatively high bandwidth requirement, and many concurrent clients. While the server limitations can be overcome by replicating the data in more nodes, the network limitations is a different challenge. Network limitations bear difficulty in determining the cause and location of congestion and in provisioning extra resources accordingly. it is shown that overlay networks can provide forward and backward secrecy for application data in an ad-hoc network. Authors present a key management and encryption scheme, called neighborhood key method, where each node shares a secret with authenticated neighbors in the ad-hoc network. The method is evaluated in a newly developed application-layer ad-hoc routing protocol. Both the ad-hoc routing protocol and the security scheme are implemented in a software system for application-layer overlay networks. Finally, through indoor and outdoor measurement experiments they evaluate the effectiveness of the neighborhood key method and the performance of application-layer ad-hoc networks.

CONCLUSION

Requirements in network management and control have been amended by emerging network and computing models. As an example, overlay networks is one emerging network application, but the new network environments and network services require new management strategies which can cope with resource constraints, scalability, dependability, context awareness, security, and mobility. Thus, the management of overlay networks should import self- management and intelligent strategies to deal with the complex management tasks. The management issues which are discussed in this paper will probably be supplemented by new approaches. It is predictable that new requirements of expanded applications will

stimulate the evolution of overlay networks, technology improvement and related management in overlay networks. In addition, there have been studied other different issues related to overlay networks in this paper, like the specific management of P2P networks, VPNs and a comparison between them, the challenges of overlay multicast and the problem of the overlay service topology design. Likewise, the topic of massive content distribution on overlay networks has been addressed as well as the overlay-based failure detection and recovery process and the issue of automating overlay network management. Furthermore, some application-layer overlay protocols have been considered for enhancing delivery services in mobile ad-hoc networks.

REFERENCES

[1] N.M. Mosharaf Kabir Chowdhury and R. Boutaba, (2009). “Network Virtualization: State of the Art and Research Challenges”. IEEE Communications Magazine , Vol. 47, Issue 7, pp20-26.

[2] D. Doval and D. O’Mahony, (2003). “Overlay Networks: A Scalable Alternative for P2P”. IEEE Internet Computing , Vol. 7, No. 4, pp79-82.

[3] M. Hofmann and L.R. Beaumont, (2005). “Content networking: architecture, protocols, and practice”. Morgan Kaufmann, ISBN: 1558608346.

[4] H. De Meer and C. Koppen, (2005). “Self-Organization in Peer-to-Peer Systems”. R. Steinmetz and K. Wehrle (Eds.): P2P Systems and Applications , LNCS 3485, pp247-266.

[5] L. Paschoal Gaspary, M.P. Barcellos, A. Detsch and R.S. Antunes, (2007). “Flexible security in peer-to-peer applications: Enabling new opportunities beyond file sharing”. Computer Networks , Vol. 51, Issue 17, pp4797-4815.

[6] R. Boutaba and A. Marshalla, (2006). “Management in peer-to-peer systems: Trust, reputation and security”. Computer Networks , Vol. 50, Issue 4, pp469-471.

[7] L. Lamport, R. Shostak and M. Pease, (1982). “The Byzantine Generals Problem”. ACM Transactions on Programming Languages and Systems , Vol. 4, No. 3, pp382-401.