ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2021;6(2):45-47

RESEARCH ARTICLE

A Survey on Secure Routing Protocol for Data Transmission in *ad hoc* Networks

B. R. Sahana

Department of CSE, VVIET, Mysuru, Karnataka, India

Received on: 05-03-2021; Revised on: 15-05-2021; Accepted on: 10-06-2021

ABSTRACT

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network. Mobile *ad hoc* network (MANET) is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. These nodes change position frequently. An *ad hoc* network can change locations and configure itself on the fly. Attacking the routing process can result in a crash of router or a severe degradation of service. Securing these routers in *ad hoc* Networks is a big issue. This paper surveys some of the techniques that how to secure the MANET followed by the methods to enhance the security level. This paper also discusses about the different protocols used to secure the *ad hoc* networks.

Key words: Computer network, Routing protocol, Ad-hoc network, MANET, Data transmission, End-to-end security

INTORDUCTION

Most routing protocols for *ad hoc* network were originally designed without having security in mind. It is specified that all nodes in network without securing the routing protocol are not sufficient. This networks with security needs, there must be two security systems; one to protect the data transmission; and one to make the routing protocol secure.[1] Securing *ad hoc* routing presents challenges because each user brings to the network with their own mobile unit, without the centralized policy or control of a traditional network. We need to solve these security related issues using some of the suitable techniques available and secure the *ad hoc* routing protocol. *Ad-hoc* on-demand distance vector (AODV) is a technique which is used to solve these security issues. The rest of the paper discusses some of the securing techniques to secure the *ad hoc* networks for data transmission.

Address for correspondence:
B. R. Sahana,
E-mail: sahana3lok@gmail.com

Survey

I. A secure routing protocol for ad hoc networks

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing security has received varying levels of attention over the past several years. Attacking the routing process can result in a crash of router or a severe degradation of service. The routing protocol attack could launched to stop the routing process from functioning properly.[2] The author of this paper examines security threats against *ad hoc* routing protocols by examining AODV Routing Protocol and dynamic source routing protocol. From these threats, they identify three different environments with distinct security requirements. They have proposed a solution for one that is managed-open scenario where no network infrastructure is pre deployed, but a small amount of prior security coordination is expected. Authenticated routing for *ad hoc* networks (ARAN), which detects and protects against malicious actions by the third parties in one particular *ad hoc* environment. This introduces authentication, message integrity and non-repudiation to an *ad hoc* environment. This has minimal performance cost for the increased security in terms of processing and networking overhead. Existing *ad hoc* routing protocols are subject to a variety of attacks that can allow attackers to influence a victim's selection of routers or enable denial of service attacks. The protocol ARAN successfully defeats all identified attacks and provides a solution for security routing in managed-open environment. In this paper, the author demonstrate exploits that are possible against *ad hoc* routing protocols, they define various security environments and offers a secure solution with an authenticated routing protocol.

II. End-to-end security implementation using transport layer security (TLS) protocol

End-to-End security has been emerging need for mobile devices with the widespread use of personal digital assistants (PDA) and mobile phones. With more and more network connected application, security has become one of the most popular concepts in mobile community. Mobile networks are open to many kind of attacks. The open data communication in these networks may cause against the security, integrity, and authenticity of data. TLS protocol is an end-to-end security protocol, commonly used on the internet together with SSL protocol.[3] Main design goals of mobile end-to-end security protocol are maintainability and extensibility. Cryptographic operations are performed with a free library, bouncy castle cryptography package. This paper presents a solution to end-to-end security needs of mobile devices, such as PDAs and mobile phones. The author of this paper concluded that communication between mobile and fixed network create particular problems can be minimized through the implementation of end-to-end security in this proxy based environment. End-to-end security solution presented in this paper is implemented for mobile devices using JAVA platform to show that it is possible and efficient to use TLS in mobile network. The work guarantees the security of any transmission at most much as TLS.

III. Optimized Link State Routing Protocol for ad hoc Networks

Link state routing protocols are one of the two main classes of routing protocols used in packet switching networks for computer communication and distance-vector routing protocol.[4] With an advent of new technologies and demand for the flexibility and ease in working environment, the use of mobile wireless computing is growing fast. As the network size increases, it becomes common for the nodes to be dispersed in a layer area for the radio range of individual nodes. In this condition, a routing technique has to be employed such that the out of range nodes may communicate with each other through intermediate nodes. The problems of routing in mobile *ad hoc* network (MANET) are been discussed in this paper. The author proposes and discusses an optimized link state routing protocol, named OLSR, for mobile wireless networks. The protocol is based on the link state algorithm and it is proactive in nature. It employs periodic exchange of messages to maintain topology information of the network at each node. It is an optimization over pure link state protocol as it compacts the size of the information sent in the messages and reduces number of retransmission to flood these messages. It provides optimal routes in terms of number of hops, which are immediately available when needed. This protocol is best suited for large and dense *ad hoc* networks. It reduces the size of the control packets instead of all links. It minimizes flooding of this control traffic using only the selected nodes called multipoint relays.

IV. Secure end-to-end data transmission in multipath routing protocol

Ad hoc networks often defined as an infrastructure less network. Without the usual routing infrastructure such as fixed routers and routing backbones. Typically, the *ad hoc* nodes are mobile and the underlying communication medium is wireless. Each *ad hoc* node may be capable of acting as a router. Some aspect of *ad hoc* network has security problems. Routing is one such aspect. The author of this paper considers the security of routing protocols for *ad hoc* networks. They use AODV routing protocol and develop a security mechanism to protect its routing information. AODV is a reactive routing protocol for *ad hoc* and mobile networks that maintains routes only between nodes which need to communicate. The routing messages do not contain information about the whole route path, but only about the source and destination. It uses destination sequence number to specify how fresh a route is and which is used to grant loop freedom. Two mechanisms are used to secure the AODV messages, Digital signatures to authenticate the non-mutable fields of messages and hash chain to secure the hop count information. For the secure AODV operations, the author suggests to look at the secure AODV routing method.

V. Secure message transmission (SMT) in MANET

Secure communication is an important aspect of any networking environment and it is a significant challenge in *ad hoc* networks. MANET paradigm seeks to enable communication across networks whose topology and membership can change frequently. Its distinctive feature is that network nodes need to collaborate with their peers in supporting the network functionality. In environment, malicious or selfish nodes can disrupt or even deny the communication of potentially any node within the *ad hoc* network domain.[5] The challenges in addressing these security vulnerabilities is due to the characteristics of MANET. The author of this paper proposes the SMT protocol to safeguard the data transmission against arbitrary malicious behavior of network nodes. SMT is a lightweight and effective protocol that can operate solely in an end-to-end manner. It exploits redundancy of multi-path routing and adapts its operation to remain efficient and effective even in highly adverse environment. SMT is better suited to support quality of service for real time communication in the *ad hoc* environment. SMT protocol to secure data forwarding operation for MANET routing protocol takes advantage of topological and transmission redundancies and utilizes feedback, exchanged between the two communication end-nodes. SMT remains effective even under highly adverse condition. The author confirms that SMT can naturally complement protocols that secure the route discovery and can shield the network operation from adversarial behavior by delivering up to 83% more data packs as compared with protocol that lack the secure data transmission feature.

CONCLUSION

Ad hoc routers can be secured using various techniques available; hence, we tend to use different protocols which may provide better security while transferring the data using routers. The paper discusses about some of the securing mechanism in different networks. The securing protocols are not only limited to fight against arbitrary malicious behavior of the nodes, they are also efficient and effective protocols that can operate solely in an end-to-end manner.[5] These securing mechanisms can be enhanced so that they can adapt its operation to remain efficient and effective even in highly adverse environment.

REFERENCES

1. Security in Mobile Ad Hoc Networks; 2015. Available from: http://www.research.ac.upc.edu/compnet/saodv.html. [Last accessed on 2015 Dec 10].
2. Security Techtarget. Routing Protocol Security; 2015. Available from: https://www.google.co.in. [Last accessed on 2015 Dec 10].
3. Transport Layer Security-Wikipedia-the Free Encyclopedia; 2015. Available from: https://www.en.wikipedia.org/wiki/Transport_layer_security. [Last accessed on 2015 Dec 10].
4. Link State Routing Protocol-Wikipedia, the Free Encyclopedia; 2015. Available from: http://www.en.wikipedia.org/wiki/Link-State-Routing-Protocol. [Last accessed on 2015 Dec 10].
5. Secure Message Transmission in Mobile ad HOC Networks; 2015. Available from: http://www.infoscience.epfl.ch/record/124938. [Last accessed on 2015 Dec 10].