Asian Journal of Multidisciplinary Research (AJMR) 2017

E-ISSN: 2395-1710 P-ISSN: 2395-1729
Volume 03- Issue02 -, pp-21-23

Research Paper Open Access

SEMI MARKOV BASED DECISION MODEL FOR GRAY HOLE ATTACK IN MANET

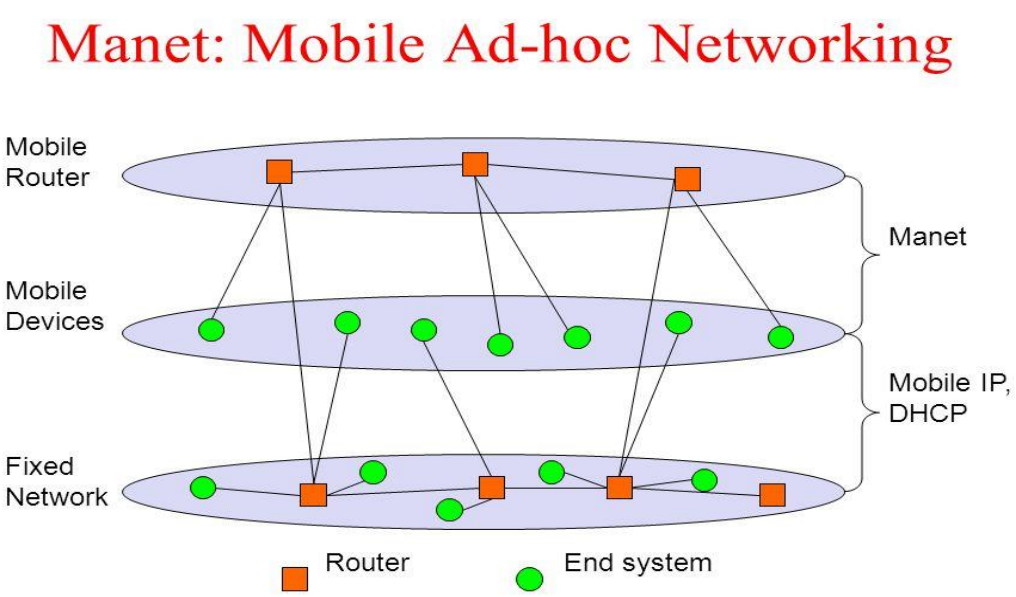
Dr.N.Danapaquiame[1] Soundarya.T[2], Bharathi.B[3], Darshani.N[4], Revathy.C[5]
Department of CSE[1,2,3,4,5], Sri Manakula Vinayagar Engineering College,
n.danapaquiame@gmail.com[1], soundhi.thaniga@gmail.com[2]
bharathibalu17@gmail.com[3], nsdarshini1995@gmail.com 4, revathy17494@gmail.com[5]

Abstract

An ad-hoc network is a LAN through which individual network nodes forward packets to and from each other. In the existing Ad-Hoc network, receiver cooperation in topology control is used to improve energy efficiency as well as network connectivity. But, the existing system does not employ distributed topology in receiver cooperation. To overcome this issue of centralized topology in the existing system, the proposed system presents an alternative based on the distributed cooperative topology control system.

Introduction

MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET.



Related works

Jamal Toutouh, José García-Nieto, and Enrique Alba ," Intelligent OLSR Routing Protocol Optimization for VANETs ",addressed the optimal parameter tuning of the OLSR routing protocol to be used in VANETs by using an automatic optimization tool. The optimization methodology presented in this paper (coupling metaheuristics and a simulator) offers the possibility of automatically and efficiently customizing any protocol for any VANET scenario, we are currently extending our experiments with new still larger urban and highway VANET instances.Jing Liu, Fei Fu, Junmo Xiao and Yang Lu PLA University of Science and Technology, "Secure Routing for Mobile Ad Hoc Networks", presents a new attack named manin-the-middle attack on EndairA. In order to prevent this attack, a new secure routing protocol, named EndairALoc, was proposed. The analysis result shows that our protocol not only retains the security. Furthermore, EndairALoc uses the symmetrical key mechanism instead of the public key mechanism, so the energy consumption in the route discovery is decreased greatly. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai," Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", , we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative blackhole attacks. Our simulation results revealed chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio.Nadav Schweitzer , Ariel Stulman, Asaf Shabtai and Roy David Margalit "Mitigating denial of service attacks in OLSR protocol using fictitious nodes" addressed that the major DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim. In this paper, they suggest a novel solution to defend the OLSR protocol from node

isolation attack by employing the same tactics used by the attack itself.

Research directions

The existing system incorporates centralized system which requires a base station to transfer data from source to destination. It does not employ distributed topology in receiver cooperation and thus does not accommodate more number of users to its network; The centralized topology is prone to transmission delay and thus faces decrease in response time. The existing system consumes more power in order to increase network connectivity. The centralized topology control scheme guarantees only one connected neighbor for each node, the network connectivity can be broken even when only a single link is disconnected.

Discussion

In the existing Ad-hoc network, receiver cooperation in topology control is used to improve energy efficiency as well as network connectivity. A node in a wireless ad-hoc network suffers from connectivity instability because of channel variation and limited battery lifespan. The centralized topology does not accommodate more number of users as it operates with the help of a base station. The existing system is prone to issues such as transmission delay, decrease in response time and high power requirement. The proposed system presents an alternative based on the distributed cooperative topology control system to overcome the issues of centralized one.The distributed system increases processing time and avoids loss of data packets in the network during transmission.The drawbacks of the existing system can be overcome by applying mutual exclusion algorithm.

Conclusion

An ad-hoc network is a LAN through which individual network nodes forward packets to and from each other. The existing system consist of an improvement algorithm for OLSR based networks (MANETs, IoT, VANETs, etc.) for mitigating gray-hole (and hence, black-hole) attacks. Using solely internal knowledge gained by participating nodes, which able to decrease captured packets by a double digit factor, using DCFM.The proposed system presents an alternative based on the semi- markov process decision model system which is used to predict the future behaviour of the current node based on which we can isolate the attacked node.

References

[1] J. Toutouh, J. Garcia-Nieto, and E. Alba, "Intelligent olsr routing protocol optimization for vanets," IEEE Transactions on Vehicular
Technology, vol. 61, no. 4, pp. 1884–1894, May 2012. [2] N. Schweitzer, A. Stulman, A. Shabtai, and R. D. Margalit, "Mitigating denial of service attacks in olsr protocol using fictitious nodes," IEEE Transactions on Mobile Computing, vol. 15, no. 1, pp. 163–172, Jan 2016.
[3] J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao, and C. F. Lai,"Defending against collaborative attacks by malicious nodes in manets:A cooperative bait detection approach," IEEE Systems Journal, vol. 9,no. 1, pp. 65–75, March 2015.
[4] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the olsr protocol," in Proceedings of Med-Hoc-Net,2003, pp. 25–27.