ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Survey on PASER - Position Aware, Secure and Efficient Routing

Tanushree Lothe

M.E. Student, Dept. of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Pune, Maharashtra, India

ABSTRACT: In disaster areas there is need of some unmanned aerial vehicles to overcome the sabotaged network. Wireless mesh network is of easy deployment and easy maintenance thus used in emergence of airborne network assisted application. Whenever needed in WMN the on-demand network access and the exploration of sized areas done efficiently. But major challenge in WMN is of security and routing attacks. That is attacker can divert the path or can drop the packet which is in result the network unnecessarily break and efficient routing is not done. As in previous work we have known the security standards 802.11i and 802.11s are vulnerable to routing attacks. Thus the security fails. There is need of secure routing protocols to make easy deployment of UAVs in WMN. Practically no any research approach accepted this because of high overhead and strong assumption. The PASER-position aware secure efficient routing gives advantage over existing approach by preventing attacks than the IEEE standards 802.11i and 802.11s used for security.

KEYWORDS: PASER, wireless network, Hop to Hop to communication, Key management

I. Introduction

In practice there is increase in humanitarian disasters and economic damages. The example of earthquake and tsunami in Japan, 1.9 million fixed telephone lines and 29000 cellular base stations were damaged. Thus disaster areas like Japan there is an emergence of restoration of whole communication network in minimum time with more efficiency over large scale. But practically it is not possible. Full restoration of communication network takes more time. The UAVs acts as a WLAN or LTE aerial hotspots to achieve this requirements. UAV helps in coverage extension and weather monitoring. To get connect UAV immediately with ground control station the internet and cellular network also needed. For this easy deployment of UAVs the airborne mesh network is used. WMN provides self-healing and auto-configuring characteristics.

II. Related work

In [1] WMN has capability of self-healing and auto-configuring which reduces network complexity and maintenance. Because of this WMN become backbone to routing attacks like black-hole attacks and wormhole attacks. Thus, an attacker may redirect the traffic or may drop the data packets even when all the backbone links are encrypted. In [2] authors referred way to strengthen the communication network against future disasters. Communication network infrastructure is an indispensable base for people’s lives and social/economic activities. The Great East Japan Earthquake and following tsunami on March 11, 2011, affected the people’s lives and caused serious communication disruptions in wide areas of Japan’s network. While intense efforts have been paid to its recovery, this unprecedented disaster have arisen serious discussions on exploring a way to strengthen the communication network against future disasters. After the earthquake, the discussion has continued, and includes another important focal point of how to take effective measures in everyday life. This talk will discuss the impact of the earthquake and the tsunami on Japans telecommunication network, progress in its recovery efforts, as well as action plans and RD policy towards building dependable future network infrastructure. In [3] authors explored to maximize the volume of air sampled by the UAVs during an individual sampling mission, the initialization interval must be as short as possible. The paper provides a simple, geometric method for generating candidate time optimal paths in steady winds, based on Dobbins well-known results for minimum time paths of bounded curvature. The approach is used to generate paths for both UAVs, which must coordinate their motion along their respective paths in order to avoid collision. The described methods were tested

DOI: 10.15680/IJIRCCE.2016. 0411086

during an aerobiological sampling experiment focusing on the plant pathogen Phytophthorainfestans. In [4] authors explained due to unique characteristics, such as dynamic network topology, limited bandwidth, and limited battery power. Routing in a MANET is a particularly challenging task compared to a conventional network. Early work in MANET research has mainly focused on developing an efficient routing mechanism in such a highly dynamic and resource-constrained network. At present, several efficient routing protocols have been proposed for MANET. In [5] authors researched that in multi-hop wireless ad hoc networks, mobile nodes cooper- ate to form a network without using any infrastructure such as access points or base stations. Instead, the mobile nodes forward packets for each other, allowing communication among nodes outside wireless transmission range. The nodes mobility and the fundamentally limited capacity of the wireless medium, together with wireless transmission effects such as attenuation, multipath propagation, and interference, combine to create significant challenges for routing protocols operating in an ad hoc network. In [6] authors explored that wireless Mesh Networks (WMNs) have been a major research focus in the recent years leading to a profusion of protocol proposals. While most existing implementations address routing aspects, none of the proposals addressing security aspects have gained acceptance in practice, due to their high overhead or strong assumptions. To cope with security issues in current WMN deployments, well-known non-secure routing protocols such as HWMP, BATMAN or OLSR could be combined with the security frameworks of the IEEE802.11s or the IEEE802.11i standards. In [7] authors explained, in emergency and rescue operations, wireless mesh networks are attracting increased attention as a high-performance and low-cost solution for ubiquitous network access. Here, the novel secure mesh route discovery protocol PASER, which has been designed to address the mesh network security in such critical environments. The protocol aims to set up reliable ad-hoc routes between network nodes and to combat unauthorized nodes of manipulating the route look-up process. Especially, its light-weight symmetric authentication scheme is noteworthy. In [8] authors says initial work in ad hoc routing has considered only the problem of providing efficient mechanisms finding paths in very dynamic networks, without considering security. Because of this, there are a number of attacks that can be used to manipulate the routing in an ad hoc network. Thus describe these threats, specifically showing their effects on ad hoc on-demand distance vector and dynamic source routing.

III. ADVANTAGES

1. Use of a secure mesh routing protocol
2. Find route discovery delay
3. Secure node to node communication
4. Reduce PASER mitigates in UAV-WMN more attacks than its alternatives
5. PASER achieves performance comparable to that of HWMPS

IV. CONCLUSION AND FUTURE WORK

This paper proposed PASER secure routing approach in UAV- WMN. Here, discussed attacks in ad-hoc network and security aspects in PASER. PASER reduces in the different case more attacks than the well-known secure routing protocol and the standardized security mechanisms of IEEE 802.11s/i. It can be used at broad range.

REFERENCES

1. Mohamad Sbeiti and Daniel Behnke, “PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks”, IEEE Transaction on Wireless Communication, vol. 15, no. 3 March 2016.
2. I. Sugino, “Disaster recovery and the RD policy in Japans telecommunication networks”, in Proc. Opt. Fiber Commun. Conf. Expo. /Nat. Fiber Optic Eng. Conf. (OFC/OFOEC), 2012.
3. L. Techy, C. Woolsey, and D. Schmale, “Path planning for efficient UAV coordination in aerobiological sampling missions”, in Proc. IEEE Decision Control (CDC), 2008, pp. 28142819.
4. L. Abusalah, A. Khokhar and M. Guizani, “A survey of secure mobile ad-hoc routing protocols”, IEEE Commun. Surveys Tuts. vol. 10, no. 4, pp. 78–93, Jan. 2008.
5. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, “A survey of routing attacks in mobile ad hoc networks”, IEEE Wireless Commun., vol. 14, no. 5, pp. 8591, Oct. 2007.
6. M. Sbeiti and C. Wietfeld, “One stone two birds: on the security and routing in wireless mesh networks”, in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), 2014, pp. 24862491.
7. M. Sbeiti, J. Pojda, and C. Wietfeld, “Performance evaluation of PASER An efficient secure route discovery approach for wireless mesh networks”, in Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC), 2012, pp. 745751

8. K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, “Authenticated routing for ad hoc networks”, IEEE J.Sel. Areas Commun. vol. 23, no. 3, pp. 598610, Mar. 2005.
9. S. Zhao, R. Kent, and A. Aggarwal, “A key management and secure routing integrated framework for mobile ad-hoc networks”, Ad Hoc Netw., vol. 11, no. 3, pp. 1046–1061, 2013.
10. Yanchao Zhang and Yanchao Zhang, “ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks”, IEEE journal on selected areas in communications, vol. 24, no. 10, October 2006.
11. T. Clausen, C. Dearlove, and J. Dean, “Mobile ad hoc network (MANET) neighborhood discovery protocol (NHDP)”, RFC 6130. Status: Standards Track. Stream: IETF, 2011.
12. Rupinder Kaur1 and Parminder Singh, Review of Black Hole and Grey Hole Attack”, the international journal of multimedia & its applications (IJMA) vol.6, no.6, December 2014.

BIOGRAPHY

Tanushree Arvind Lothe is a Student in the Computer Engineering Department (Computer Networks), Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India. She received Bachelor of Electronics and Telecommunication Engineering (BE) degree in 2014 from NDMVP COE, Nashik, Maharashtra, India. Her research interests are Computer Networks (wireless networks) and Network Security.

DOI: 10.15680/IJIRCCE.2016. 0411086