International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 07th Jan 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=ISSUE-1

DOI: 10.48047/IJIEMR/V12/ISSUE 01/55

Title Safe and Efficient Airborne Mesh Network Routing (PASER)

Volume 12, Issue 1, Pages: 589-596

Paper Authors
Mrs. S.Lalitha, M.Chandana, M.Vijaya Durga, S.Niharika

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Safe and Efficient Airborne Mesh Network Routing (PASER)

Mrs. S.Lalitha,Assistant Professor, Dept. of Information Technology, Sridevi Women's Engineering College, Hyd. Shudulalalitha@gmail.com

M.Chandana, B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

M.Vijaya Durga, B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

S.Niharika, B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

ABSTRACT— The advent of network-assisted applications in the air has been aided by the combination of low-altitude Unmanned Aerial Vehicles (UAVs) and WLAN Mesh Networks (WMNs). InDuring times of crisis, these technologies are indispensable for facilitating I instantaneous, ubiquitous network connection and (ii) productive, sized-area exploration.

Nonetheless, there are still significant security issues with these systems since WMNs are vulnerable to routing attacks. As a result, attacks on the network are possible, and the bad guys may even take control of the UAVs or tamper with the payload information. Previous research of ours experimentally shown the susceptibility of modern security standards to routing attacks, including the IEEE 802.11i and the security procedures of the IEEE 802.11s mesh standard. To this end, a trustworthy routing protocol is crucial for UAV-practical WMN's implementation. Due to their large overhead or strong assumptions, none of the current research methodologies have acquired adoption in practise, as far as we are aware. With this paper, we introduce Position-Aware, Secure, and Efficient mesh Routing (PASER). Unlike the IEEE 802.11s/i security mechanisms and the popular, secure routing system ARAN, our solution does not impose artificial limitations on network design.Compared to the well-established, non-secure routing technology HWMP paired with the IEEE 802.11s security features, PASER provides comparable performance results in actual UAV-WMN situations.

INTRODUCTION

According to the latest global assessment report on disaster risk reduction from the United Nations, the number of natural disasters worldwide has been on the rise.recent years have seen an increase in the frequency and severity of natural catastrophes, causing more human suffering and economic devastation. The paper notes that the loss of communication is a major issue in disaster zones. Specifically, Sugino claims that 1.9 million fixed telephone lines and 29,000 cellular base stations were destroyed during the big east Japan earthquake and tsunami in March 2011. He adds that although emergency repairs to the communication networks only took a month, the overall repair process took 11 months. All of this points to the growing significance of mobile communication systems in disaster zones. In addition, these numbers demonstrate that a communication

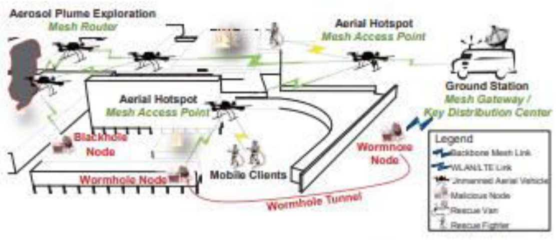


Fig. 1. Example of a deployment scenario of UAV-WMN and two routing attacks in disaster relief.

A network that doesn't depend on preexisting infrastructure and can be created in a very short amount of time (say, an hour) is crucial for effectively handling massive events.crises. These criteria are satisfied by low-altitude, autonomous Unmanned Aerial Vehicles (UAVs) serving as WLAN or LTE aerial hotspots . As an added bonus, the UAVs may be fitted with sensors allowing collaborative study of circumstances where unchecked discharges of liquid or gaseous toxins occur. Additionally, UAVs have been used in applications such as coverage extension/densification [6], precision farming [7], and polar weather monitoring [8]. In spite of this, for such applications to materialise, a trustworthy, auto-configuring, and self-healing wireless backbone network is required to link the UAVs together and to connect them to their ground control station, the Internet, and the cellular core network. Due to its compatibility with the aforementioned features [9], as well as their provision of a physical air-to-air connection for direct communication between the UAVs, Wireless Mesh Networks (WMNs) are a promising option.As shown in Fig. 1, UAVs linked together by means of a WMN (UAV-WMN) may form an aerial mesh network that can aid in disaster relief efforts. The UAVs, as seen in the image, work together to create a mobile wireless mesh backbone. This infrastructure can provide network coverage to legacy mobile WLAN/LTE clients (devices used by rescue workers) on demand. It addresses issues related to the open transfer of data between the UAVs and their customers, including data gathered by the UAVs' sensors.

RELATED WORK

"On the Security and Routing in Wireless Mesh Networks, One Stone, Two Birds"

Recent years have seen an explosion of protocol ideas for Wireless Mesh Networks (WMNs), the subject of intensive study. However, owing to their significant cost or strong assumptions, none of the ideas addressing security concerns have received practical adoption while current implementations focus on routing. Well-known insecure routing protocols like HWMP, BATMAN, or OLSR might be integrated with the security frameworks of the IEEE802.11s or the IEEE802.11i standards to deal with security vulnerabilities in present WMN installations. In this study, we compare and contrast the two security frameworks and examine their effects on WMN performance in both simulated and real-world settings. Further, we demonstrate empirically that neither framework protects against blackhole or wormhole assaults. Furthermore, we show that a dynamic key management scheme and an effective secure routing protocol are required to set up dependable WMNs.

“The Anguish of Having to Decide: A Study of Routing Protocols for Chained-Mesh Networks”

In recent years, researchers have focused their attention on improving the routing in wireless mesh networks, resulting to an explosion of proposed protocols.

In reality, determining which protocol to use and how to best set its parameters for a specific network are two of the most difficult tasks. In the present study

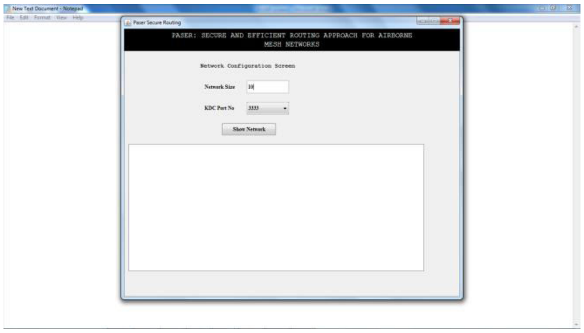
compares PASER, a safe routing protocol, against some of the most popular insecure routing protocols, including OLSR, BATMAN, and HWMP, and finds that chain mesh networks have advantages over both. Parameter optimizations are produced after a comprehensive investigation of the protocols' behaviour. The findings support the superior performance of reactive or hybrid routing strategies over proactive routing techniques in chain mesh networks with static source-destination pairs and an average number of forwarding hops. If network security is not a priority, then HWMP is the best option for such systems. Alternatively, as we empirically demonstrate, PASER is a better option owing to security weaknesses in the IEEE802.11 security frameworks.

METHODOLOGY

The PASER method makes the following assumptions about the network and the adversary.Network Model, No. 1: PASER takes into account a mobile-centric wireless mesh backbone as its intended network (UAV)

nodes, and one fixed (ground station) node. Here, we presume that the network is controlled by a single entity (such as fire departments), making it difficult to join. All legitimate operator nodes adhere to the system protocols, however malevolent nodes may break the rules. Network operators are expected to be the certifying authority in a public key infrastructure. Valid nodes are identified by a certificate that specifies their responsibilities (gateway, access point, or router). In order to dynamically manage network credentials, the network operator operates a secure Key Distribution Center (KDC).The KDC's public key is distributed to every node. Mesh gateways can reliably connect to the KDC and vice versa at any moment. To do this with UAV-WMN, the KDC is often conducted from a stationary location. A positioning device providing a private navigation service, like Galileo's Public Regulated Service, is presumed to be a part of the valid nodes. In other words, much as in UAV-WMN, the goal scenario is anticipated to take place in the great outdoors and have few barriers.(2) The Attacker Model: This study focuses on threats to routing security. The primary goal of the attacker is to compromise the flight security of the UAVs by manipulating the routes, hence disrupting the network or launching sophisticated assaults. The attacker is thought to be in charge of many untrusted nodes that might potentially outperform the trusted ones in terms of resources and connectivity. The attacker may use social engineering, physical assaults, cryptanalysis, or other techniques to compromise legitimate nodes or network credentials. This allows the attacker to use the stolen identities and keys to pose as genuine network nodes. The attacker might cause nodes under his control to behave inconsistently with the protocol.Specifically, they may cause data loss, packet alterations, or routing message corruption. In addition to acting in unison, attacking nodes have access to many lines of communication that allow them to coordinate their efforts from far away. But the adversary's computing capabilities are limited, so they can't crack the simplest forms of crypto. The most important assaults, according to our adversary model, are shown in Table II below. Both external and internal threats are distinguished. Assuming the former, the attacker is cut off from the system. In the latter scenario, assaults are carried out after genuine network credentials have been leaked or a trusted node has been compromised.

RESULT AND DISCUSSION



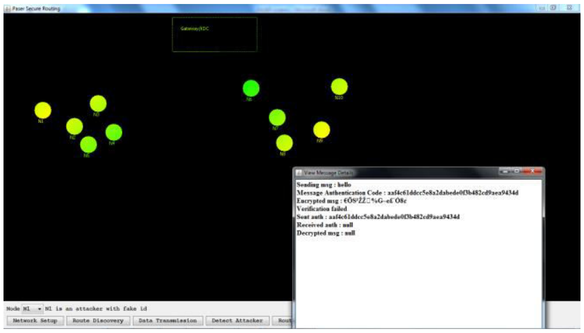
PASER: SECURE AND EFFICIENT ROUTING APPROACH FOR AIRBORNE MESH NETWORKS

Network Configuration Screen

Network Size: 10

KDC Port No: 3333

To begin, pick the KDC port number and then enter the network size (the total number of nodes) (on which the KDC server is running)

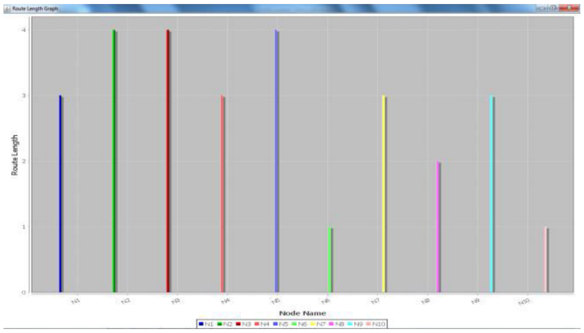


View Message Details

```
Sending msg : hello
Message Authentication Code : aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d
Encrypted msg : €ÕS²ŽŽ□%G–e£˙Õ8c
Verification failed
Sent auth : aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d
Received auth : null
Decrypted msg : null
```

Node N1 ▾ N1 is an attacker with fake id

Upon receiving a key from the KDC, the node may then connect to the gateway.



CONCLUSION

In order to ensure the safety of UAV-WMN traffic, this study examines the PASER secure routing method. In the circumstances studied, PASER is found to be more effective in mitigating assaults than the more conventional,

ARAN, a secure routing technology, and the IEEE 802.11s/i security standards. A theoretical and simulated examination of PASER's route discovery process is conducted to investigate its efficacy, and the routing algorithm's scalability with regard to network size and traffic load is rationalised. In UAV-WMN-assisted network provisioning and area exploration scenarios, it is shown that PASER's performance is on par with that of the well-established, none-secure routing protocol HWMP combined with the IEEE 802.11s security mechanisms using the network simulator OMNeT++, realistic mobility patterns of UAVs, and a channel model of UAV-WMN derived from experiments. In conclusion, PASER's advantages have been recently demonstrated at several events, including the Vodafone innovation days 2014 [76], and its OMNeT++ and Linux implementations may be found at www.paser.info. We want to expand our examination of PASER's potential uses in the near future.

REFERENCES

[1] (2015) Flying New Way, RPAS, A Boost for European Creativity and Innovation. European Commission. [Online]. Available: http://ec.europa.eu/growth/flipbook/rpas/?goback=.gde

[2] (2015) Global Assessment Report on Disaster Risk Reduction. United Nations (UN). [Online]. Available:

[3] I. Sugino, "Disaster Recovery and the R&D Policy in JapanŠs Telecommunication Networks," in Plenary Talk at OFC/OFOEC, 2012. [4] (2015) Facebook Will Deliver Internet Via Drones. J. Constine, TechCrunch. [Online]. Available: http://techcrunch.com/2014/03/27/facebook-drones/

[5] C. Wietfeld and K. Daniel, "Cognitive Networking for UAV Swarms," in Handbook of Unmanned Aerial Vehicles, K. P. Valavanis and G. J. Vachtsevanos, Eds. Springer, 2014.

[6] A. Abdulla, Z. Md Fadlullah, H. Nishiyama, N. Kato, F. Ono, and R. Miura, "Toward Fair Maximization of Energy Efficiency in Multiple UAS-Aided Networks: A Game-Theoretic Methodology," IEEE Transactions on Wireless Communications, vol. 14, no. 1, 2015.

[7] L. Techy, C. Woolsey, and D. Schmale, "Path Planning for Efficient UAV Coordination in Aerobiological Sampling Missions," in IEEE CDC, 2008.

[8] J. Curry, J. Maslanik, G. Holland, and J. Pinto, "Applications of Aerosondes in the Arctic," Bulletin of the American Meteorological Society, vol. 85, no. 12, 2004.

[9] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," Elsevier Computer Networks, vol. 47, no. 4, 2005.

[10] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A Survey of Routing Attacks in Mobile Ad hoc Networks," IEEE Wireless Communications, vol. 14, no. 5, 2007. [11] (2015) New Rules for Small Unmanned Aircraft Systems. Federal Aviation Administration, U.S. Department of Transportation. [Online]. Available: http://www.faa.gov/news/press_releases/news_-story.cfm?newsId=18295

[12] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)

Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Std 802.11, 2004.

[13] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11, 2012. [14] M. Sbeiti and C. Wietfeld, "One Stone Two Birds: On the Security and Routing in Wireless Mesh Networks," in IEEE WCNC, 2014.

[15] ——, "The Agony of Choice: Behaviour Analysis of Routing Protocols in Chain Mesh Networks," in Springer Lecture Notes on Ad Hoc Networks, 2014, vol. 129.

[16] H. Y. and A. Perrig, "A Survey of Secure Wireless Ad hoc Routing," IEEE Security and Privacy, vol. 2, no. 3, 2004.

[17] L. Abusalah, A. Khokhar, and M. Guizani, "A Survey of Secure Mobile Ad hoc Routing Protocols," IEEE Communications Surveys and Tutorials, vol. 10, no. 4, 2008.

[18] (2015) AIRBorne information for Emergency situation Awareness and Monitoring (AIRBEAM). [Online]. Available: http://airbeam.eu/project/

[19] (2015) UAV-Assisted Ad Hoc Networks for Crisis Management and Hostile Environment Sensing (ANCHORS). [Online]. Available: http://anchors-project.org/index.php/en/

[20] M. Sbeiti, J. Pojda, and C. Wietfeld, "Performance Evaluation of PASER - an Efficient Secure Route Discovery Approach for Wireless Mesh Networks," in IEEE PIMRC, 2012.

[21] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated Routing for Ad hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 23, 2005.

[22] (2015) Better Approach To Mobile Ad hoc Networking (B.A.T.M.A.N.). Freifunk Community. [Online]. Available: http://www.open-mesh.org/

[23] (2015) Wireless Battle Mesh. [Online]. Available: http://battlemesh.org/AboutUs

[24] G. Lebovitz and M. Bhatia, "Keying and Authentication for Routing Protocols (KARP) Design Guidelines," RFC 6518. Status: Infomational. Stream: IETF, 2012.

[25] A. Sgora, D. Vergados, and P. Chatzimisios, "A Survey on Security and Privacy Issues in Wireless Mesh Networks," Wiley Online Library Security and Communication Networks, 2013. [26] J. Sen, "Security and Privacy Issues in Wireless Mesh Networks: A Survey," CoRR, vol. abs/1302.0939, 2013.

[27] A. Naveed, S. Kanhere, and S. Jha, "Attacks and Security Mechanisms," in Security in Wireless Mesh Networks, Y. Zhang, J. Zheng, and H. Hu, Eds. Auerbach Publications, 2008. [28] H. Lin, J. Ma, J. Hu, and K. Yang, "PA-

SHWMP: A Privacy-Aware Secure Hybrid Wireless Mesh Protocol for IEEE 802.11s Wireless Mesh Networks," Springer EURASIP Journal on Wireless Communications and Networking, vol. 2012, no. 1, 2012.

[29] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: a Novel PrivacyEnhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 2, 2010.

[30] T. Wu, Y. Xue, and Y. Cui, "Privacy Preservation in Wireless Mesh Networks," in Security in Wireless Mesh Networks, Y. Zhang, J. Zheng, and H. Hu, Eds. Auerbach Publications, 2008.

[31] X. Wu and N. Li, "Achieving Privacy in Mesh Networks," in ACM SASN, 2006.

[32] Y. Zhang and Y. Fang, "ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 10, 2006.

[33] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of Wireless Communication Technologies for Public Safety," IEEE Communications Surveys Tutorials, vol. 16, no. 2, 2014.

[34] J. Ben-Othman and Y. Saavedra Benitez, "IBC-HWMP: a Novel Secure Identity-based Cryptography-based Scheme for Hybrid Wireless Mesh Protocol for IEEE 802.11s," Wiley Online Library on Concurrency and Computation: Practice and Experience, vol. 25, no. 5, 2013.