*International Journal of Engineering & Technology*, 7 (3.29) (2018) 697-701

SPC

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# Empirical Study on Paser for Airborne Mesh Networks using Bloom Filters

**Dr.Amjan Shaik [1*], Vaishnavi.P [2], Dr.M.Neelakantappa [3]**

*[1]Professor of CSE,[2] M.Tech CSE-Student, [3] Professor of IT*
*[1,2,3] BVRIT, TS, India.*
**Corresponding Author E-mail : amjan.sk@bvrit.ac.in*

## Abstract

Squat-altitude unmanned in-flight vehicle (UAVs) blend through WLAN system networks (WSNs) has facilitate the coming out of airborne community- assisted correspondence. In devastation remedy, they may be key solutions for 1) on-call for ubiquitous network get right of access to and 2) a pair of inexperienced exploration of sized regions. Contemporary protection standards, which includes the IEEE 802.11i and the safety appliances of the IEEE 802.11s mesh good sized, are prone (exposing routing attacker) to routing assaults as we experimentally confirmed in previous works, where in it is well-known, at ease routing protocol ARAN, lacking makes restraining conventions. Therefore, at ease routing protocol is vital for making viable the arrangement of UAV-WMN. As an extended way we realize, not one of the winning research techniques have acquired popularity in exercise because of their excessive overhead or sturdy assumptions. Here, we present the vicinity-aware, relaxed, and inexperienced mesh routing technique (PASER) with the extension of Bloom Filters. PASER achieves comparable regular overall performance results because of the nicely-set up, non-secure routing protocol HWMP (Hybrid wireless mesh protocol) collective with the IEEE 802.11s safety mechanisms. We implemented BLOOM FILTERs instead of HMAC.

***Keywords**: Routing Protocol, UAV's, UAV-WMN, Bloom Filters*

## 1. Introduction

In cryptography, an HMAC is a particular kind of Message Authentication Code (MAC) connecting a cryptographic hash representative and a undisclosed cryptographic key, used to instantaneously authenticate both the data reliability and the authentication of a message with any MAC. Any cryptographic hash function, such as MD5 or SHA-1 might be recycled in the calculation of an HMAC; the resultant MAC algorithm is termed HMAC-X, where X is the hash function recycled (e.g. HMAC-MD5 or HMAC-SHA1).Low-altitude, self sufficient Unmanned Aerial Vehicles (UAVs) performing as WLAN or LTE aerial hotspots meet these necessities. Nevertheless, for such packages to emerge as a authenticity, a trustworthy, auto-configuring, and self-restoration wireless spine network is required to interrelate the UAVs and to deliver a joining to their ground manage station, the Internet, and the cell core community [7]. Wireless Mesh Networks (WMNs) is a exact candidate as they've the aforementioned traits, and they provide a bodily air-to-air hyperlink for a direct communiqué between the UAVs [9].
Fig. 1 illustrates how an airborne mesh community such as UAVs linked via a WMN (UAVWMN) can be used to help in catastrophe comfort operations. As the discern suggests, the UAVs build a transportable wireless mesh spine. This spine gives, on call for, network insurance to legacy mobile WLAN/LTE customers (rescue fighters' devices) [10]. It additionally offers with the obvious delivery of the clients' data as well as the sensor records of the UAVs. Above these all security provided we are here by implementing Bloom filters which provides more efficient way of securing data and also helps to reduce up the efficiency.

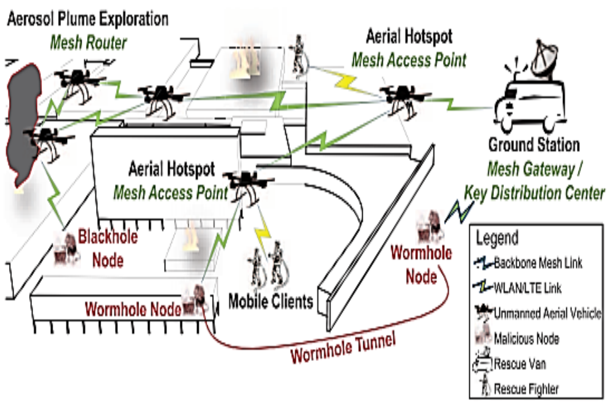


Fig. 1. Example of a deployment scenario of UAV-WMN and two routing attacks in disaster relief.

## 2. Research Background

Wireless mesh networks (WMN) have just apprehended the awareness of educational and manufacturing researcher societies; as they characterize an amazing method to supplying wireless

Internet connectivity in a tremendous geographic region.. Second, we advocate a brand new scheme, known as Selective and Deterministic Pipelined packet Marking for Mesh Networks (SDPMM). This scheme is used for IP visitors source identity for tracing denial of service (DoS) attacks. The technique follows the IP trace back method planned in wired networks [15]. Having a look it shows that SWMM outstrips additional present techniques in relations of handoff latency, loss, and blocking off price. It similarly displays that the site visitors overhead delivered through the trace back scheme does now not have an effect on the network overall performance [11]. To permit users an effective and reliable handoff, as well as a comfy get right of entry to the mesh network, a way of re-authentication, with reduced put off, must be finished at some stage in the mobility of mobile nodes over unique SMAPs and via numerous clusters. In addition, a WMN can be prone to many types of attacks, especially DoS and DDoS attacks [1]. We have additionally proposed a unique hint again method for WMNs, known as “selective and deterministic pipelined packet marking for mesh networks” (SDPMM).Recent improvements in embedded systems, energy storage, and communication interfaces convoyed by the dropping charges of WLAN routers and a significant growth in the throughput of a WLAN (IEEE 802.11) have simplified the explosion of WLAN Mesh Network (WMN) applications. For illustration, WMNs are planned to connect self-organized, cooperative, and small Unmanned Aerial Vehicles in a wide range of applications, such as emergency response, environmental monitoring, and ad-hoc network provisioning [7]. A wireless mesh network has assisted as a mainstay for the conventional order of numerous forthcoming technologies. That is conceivable due to self-recovery, vehicle-configuration nature of these networks. On one hand, it gives an comfort for compatibility, availability, feasibility however on other hand they are prone to several security attacks, which can interfere the communication between sender and receiver [6].

WMN is now a day’s providing an extensive support for IP services and upcoming technologies. Security is some of the challenging issues still exist in wireless mesh network. The work done in this paper shows the exclusion of spiteful nodes with the help of Hash RSA algorithm. The simulation of the network was done in NS2 with the effect during the DoS attack. We identified the malicious nodes and then black listed them during the routing. Hybrid cryptography was used in improving the key generation process of the Hash RSA algorithm. The results show significant improvement with the use of Hash RSA optimized with hybrid cryptography [14]. The performance was analyzed and checked on various parameters like throughput, jitter and end to end delay. It provides much greater performance and handles the security of network. For future enhancement Security feature in network has attracted many researchers[12][13]. In the future scope the implementation of algorithm can be applied in various application scenarios such as to relay the communication between UAV, deployment of IP services. Thus it will help in making wireless network furthermore reliable [9].

## 3. Methodology

PASER is pursuits to easy the routing manner in UAV-WMN in a practicable method. We first of all proposed PASER in this paper [5]. In this segment, we amplify upon our preceding works with the aid of actually defining the community and attacker models of PASER, and via extending its security desires, based on discussions with UAVWMN cease-users and stakeholders amongst others. Here, PASER has been better to offer origin authentication with the intention to proactively limit the damage of inner attackers, i.e., to fight the fabrication and black hole assaults. The dynamic key administration scheme of PASER has been accustomed to consist of the key range in all PASER messages for a improved discovery of key modifications. From the routing factor of view, the route accumulation has been eliminated as it was located that this structure is unproductive in UAV-WMN [5]. The statistics won from route gathering in UAV-WMN is well worth much fewer than the overhead it produces. Apart from that, whilst we most effective addressed the direction discovery manner in our previous works, we've upgraded PASER to consist of a path upkeep mechanism and also further work we introduced Bloom filters.

### 3.1. Bloom Filter

A Bloom filter is a space-efficient probabilistic information organization with the purpose of is used to experiment whether a component is a part of a set. The price we wage for effectiveness is that it is probabilistic in environment which means, there might be some False Positive results. False tremendous matches are viable; however false negatives are not – in different words, a query proceeds both "likely in set" or "actually not in set". Elements may be delivered to the set, however now not eliminated (even though this could be spoken with a "counting" clear out); the more factors which are delivered to the set, the bigger the chance of fake positives.

### 3.2. Constructing Bloom Filters

Consider a set of n elements. Bloom filters define membership data of a using a bit vector V of length m. For this, k hash functions, with, are used as described below:
The succeeding technique builds an m bits Bloom filter, matching to a set A and using hash functions:

**Procedure**

```
Procedure BloomFilter(set A, hash_functions, integer m)
returns filter
filter = allocate m bits modified to 0
foreach $a_i$ in A:
    foreach hash function $h_j$:
        filter[hj(ai)] = 1
    end foreach
end foreach
return filter
```

Consequently, if $a_i$ is component of a set A, in the ensuing Bloom filter V all bits obtainanalogous to the hashed principles of $a_i$ are put to 1. Testing for connection of an element elm is comparable to testing that all conforming bits of V are set:

```
Procedure MembershipTest (elm, filter, hash_functions)
 returns yes/no
foreach hash function hj: if filter[hj(elm)] != 1
    return No
end foreach
return Yes
```

### 3.3. Bloom Filters – the Math

One prominent feature of Bloom filters is that there is a clear tradeoff between the size of the filter and the rate of false positives. Detect that after introducing n keys into a filter of size m using k hash functions, the probability that a actual bit is still 0 is: .

$$p_0 = \left(1 - \frac{1}{m}\right)^{kn} \approx 1 - e^{-\frac{kn}{m}} \qquad (1)$$

(Note that we accept perfect hash functions that range the elements of A calmly through the space {1..m}. In preparation, worthy conclusions have been accomplished using MD5 and other hash functions.) Later, the probability of a false positive (the probability that all k bits have been beforehand set) is:

$$p_{err} = (1-p_0)^k = \left(1-\left(1-\frac{1}{m}\right)^{kn}\right)^k \approx \left(1-e^{-\frac{kn}{m}}\right)^k \qquad (2)$$

In (2) $p_{err}$ is minimized for $k = \frac{m}{n}\ln 2$ hash functions.

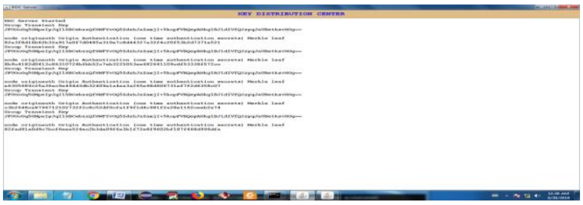
### 3.4. Bloom Filters – Algorithm

**Algorithm 1**

```
S ← Null Boolean Filter of size m
V← Hash table
for all reads udo
    for all k-mers y in u do
        $y_{rep}$ ← min(y, revcomp(y))
        if $y_{rep}$ € S then
            if $y_{rep}$ € V then
                V[$y_{rep}$] ← 0
        else
            add $y_{rep}$to S
for all reads u do
    for all k-mers yin u do
        $y_{rep}$← min(y, revcoomp(y))
        if $y_{rep}$ € V [$y_{rep}$]+1
            V[$y_{rep}$] ← V[$y_{rep}$] +1
for all y € V do
    if V[y] = 1 then
        remove y from V
```

## 4. Result Analysis

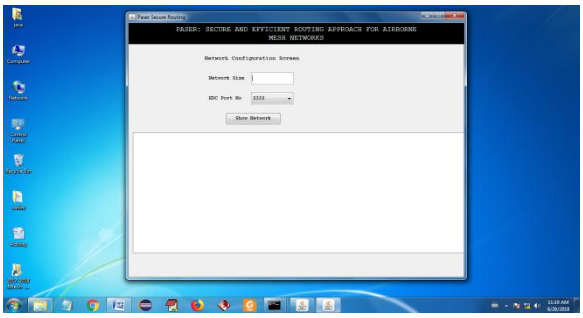
In this purpose system we introduced KDC(Key Distribution Center) and PASER Secure Routing server which used to distribute the key among all authentication node on the simulation. All nodes contact the KDC in direction to accept the network keys.


KDC Server

KEY DISTRIBUTION CENTER

```
KDC Server Started
Group Transient Key
[illegible]

node originauth Origin Authentication (one time authentication secrets) Merkle leaf
[illegible]
Group Transient Key
[illegible]

node originauth Origin Authentication (one time authentication secrets) Merkle leaf
[illegible]
Group Transient Key
[illegible]

node originauth Origin Authentication (one time authentication secrets) Merkle leaf
[illegible]
Group Transient Key
[illegible]

node originauth Origin Authentication (one time authentication secrets) Merkle leaf
[illegible]
Group Transient Key
[illegible]

node originauth Origin Authentication (one time authentication secrets) Merkle leaf
[illegible]
```

When the user enter the Network size and click on show network then only the simulation starts at paser secure routing server as well as key distribution center.


Paser Secure Routing

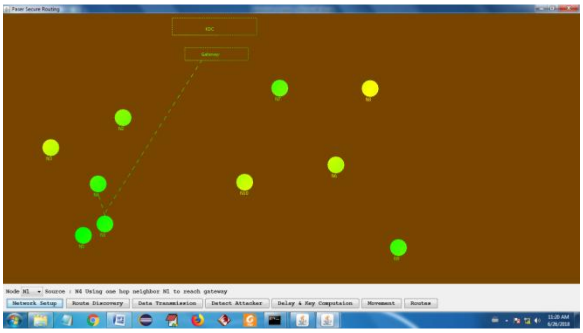
PASER: SECURE AND EFFICIENT ROUTING APPROACH FOR AIRBORNE MESH NETWORKS

Network Configuration Screen

Network Size

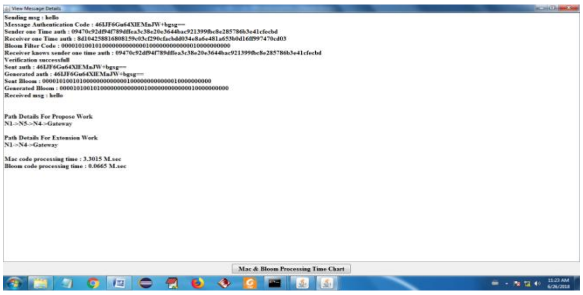
KDC Port No 3333

In the simulation screen the nodes are arranged we should set the path from source to destination.

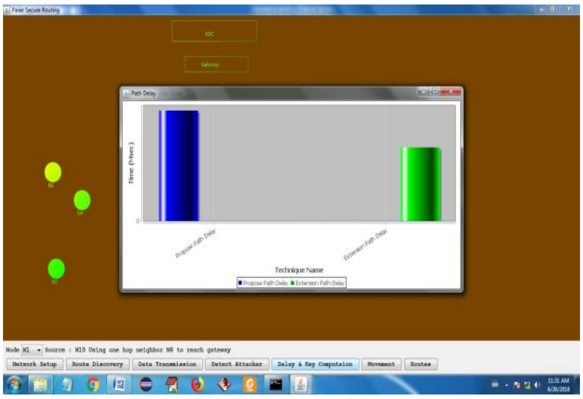


Node N1 Source : N4 Using one hop neighbor N1 to reach gateway

The details about shortest path and node details all are exhibited in the View message.

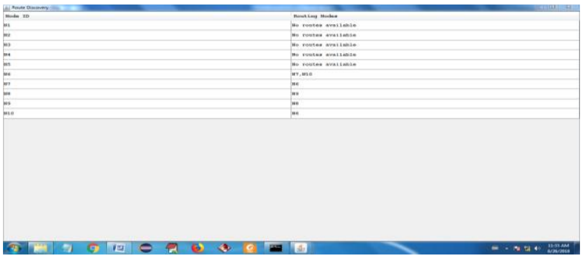

View Message Details

```
Sending msg : hello
Message Authentication Code : 46IJF6Gu64XIEMnJW+bgsg==
Sender one Time auth : 09470c92df94f789dffea3c38e20e3644bac921399fbc8e285786b3e41cfecbd
Receiver one Time auth : 8d10425881680815 9c03cf290cfacbdd034e8a6e481a653b0d16ff997470cd03
Bloom Filter Code : 000010100101000000000000001000000000000010000000000
Receiver knows sender one time auth : 09470c92df94f789dffea3c38e20e3644bac921399fbc8e285786b3e41cfecbd
Verification successfull
Sent auth : 46IJF6Gu64XIEMnJW+bgsg==
Generated auth : 46IJF6Gu64XIEMnJW+bgsg==
Sent Bloom : 000010100101000000000000001000000000000010000000000
Generated Bloom : 000010100101000000000000001000000000000010000000000
Received msg : hello


Path Details For Propose Work
N1->N5->N4->Gateway

Path Details For Extension Work
N1->N4->Gateway

Mac code processing time : 3.3015 M.sec
Bloom code processing time : 0.0665 M.sec
```



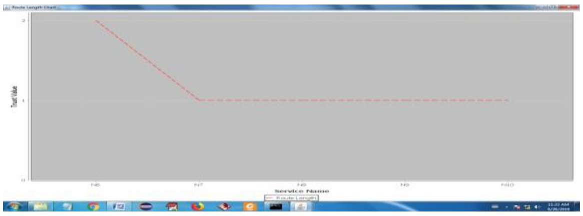
Node N1 Source : N10 Using one hop neighbor N8 to reach gateway

After that click on Movement button it find outs the available route details for all nodes. Display the available or not available routes list.

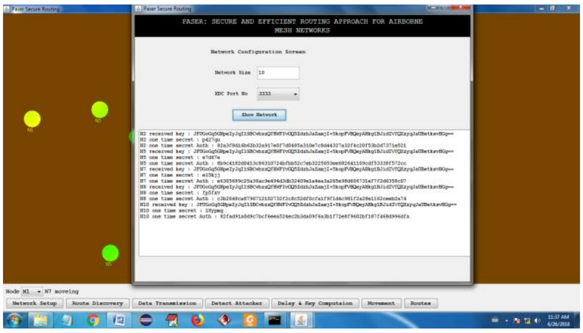

Route Discovery

| Node ID | Routing Nodes |
|---|---|
| N1 | No routes available |
| N2 | No routes available |
| N3 | No routes available |
| N4 | No routes available |
| N5 | No routes available |
| N6 | N7,N10 |
| N7 | N6 |
| N8 | N9 |
| N9 | N8 |
| N10 | N6 |

Now click on Routes button. It display the Route Length Chart for the nodes



Finally the total processing details were placed in Mesh Network & KDC servers as given below

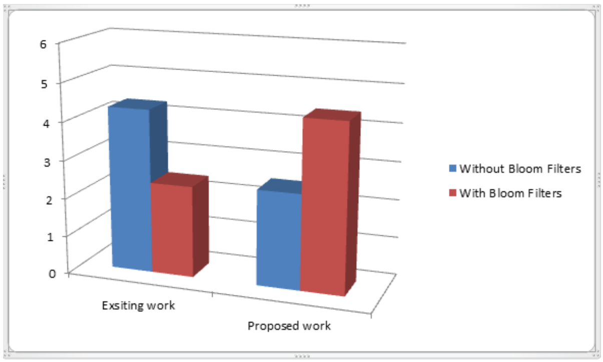


Network Size: 10

KDC Port No: 3333

```
N2 received key : JFUGoGq5GBpeIyJqI1SBCwbzzQfHWFYvOQ5ZdzhJaZamjI+5kopFVBQeyAHkg1BJidIVfQXzyqJaUBetksvHGg==
N2 one time secret : p427qu
N2 one time secret Auth : 82a3f8d16b62b32a917e0f7d0485a310e7c8d44327a32f4c20f53b0d7371e521
N5 received key : JFUGoGq5GBpeIyJqI1SBCwbzzQfHWFYvOQ5ZdzhJaZamjI+5kopFVBQeyAHkg1BJidIVfQXzyqJaUBetksvHGg==
N5 one time secret : e7d67e
N5 one time secret Auth : 8b9c4182d0413c86310724bfbb52c7eb3225053ee682641189cdf53338f572cc
N7 received key : JFUGoGq5GBpeIyJqI1SBCwbzzQfHWFYvOQ5ZdzhJaZamjI+5kopFVBQeyAHkg1BJidIVfQXzyqJaUBetksvHGg==
N7 one time secret : a15kjj
N7 one time secret Auth : e6305689c25a36ac9e494d3db32409e1a4ea3a265e98d606731ef7f2d6358c07
N8 received key : JFUGoGq5GBpeIyJqI1SBCwbzzQfHWFYvOQ5ZdzhJaZamjI+5kopFVBQeyAHkg1BJidIVfQXzyqJaUBetksvHGg==
N8 one time secret : fp5fxv
N8 one time secret Auth : c3b2648ca8796712102732f2c8c52df0cfa1f9f1d4c981f2a28e1162ceeb2a74
N10 received key : JFUGoGq5GBpeIyJqI1SBCwbzzQfHWFYvOQ5ZdzhJaZamjI+5kopFVBQeyAHkg1BJidIVfQXzyqJaUBetksvHGg==
N10 one time secret : 18ypmq
N10 one time secret Auth : 82fad91a0d9c7bcf6eea524ec2b3da09f6a3b1f72e8f9602bf187f468d996dfa
```

Below diagram shows the difference of processing time of existing and proposed work where on it shows a drastic change in the time of processing by implementation of Bloom filters.



The above diagram shows drastic change in computation between existing and proposed systems.

## 5. Conclusion

This paper analyzes the PASER secure routing method in UAV-WMN using Bloom Filter. Replacement of HMAC with this algorithm helped up to decrease the complexity and perform the analysis in efficient manner, indeed it helped to prove that PASER mitigates inside the investigated scenarios greater attacks than the well-known, cozy routing protocol ARAN and the standardized protection mechanisms of IEEE 802.11s/I, which helped performance of PASER to explore in a theoretical and simulation-primarily based analysis of its course discovery system, and its scalability with respect to network size and site visitor's load is reasoned [2]. Using the network simulator OMNeT++, realistic mobility styles of UAVs, and an experimentally derived channel version of UAV-WMN, its miles demonstrated that in UAV-WMN-assisted community provisioning and place exploration eventualities PASER has a similar performance with that of the well-mounted, none-comfy routing protocol HWMP mixed with the IEEE 802.11s safety mechanisms. Last, the benefits of PASER with bloom filters in these days provides different events, which include the Vodafone innovation days 2014, and its implementations in OMNeT++ and in Linux are to be had underneath www.Paser.Information. In destiny work, we intend to investigate the use of PASER in a broader variety of application situations.

## 6. Future Scope

As a future work we can implement Cache filters to increase space on disk. Counting filters which helps to query an elements exact value, can be implemented it with support of Bloom filters. An Attenuated Bloom Filter can also be implemented for service discovery in a network.

## Acknowledgement:

We would like to thank all authors in reference list and thankful to Dept. lab and faculty for supporting us to do this work in bright way.

## References

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

[2] United Nations (UN). (2015). Global Assessment Report on Disaster Risk Reduction [Online]. Available: http://www.preventionweb.net/english/ hyogo/gar/2013

[3] Sugino, "Disaster recovery and the R&D policy in Japans telecommunication networks," in Proc. Opt. Fiber Commun. Conf. Expo./Nat. Fiber Optic Eng. Conf. (OFC/OFOEC), 2012.

[4] J. Constine. (2015). Facebook Will Deliver Internet Via Drones, TechCrunch [Online]. Available: http://tech crunch . 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. New York, NY, USA: Springer, 2014.

[6] 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 Trans. Wireless Commun., vol. 14, no. 1, pp. 305–316, Jan. 2015.

[7] 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. 2814–2819.

[8] J. Curry, J. Maslanik, G. Holland, and J. Pinto, "Applications of aerosondes in the arctic," Bull. Amer. Meteorol. Soc., vol. 85, no. 12, pp. 1855–1861, 2004.

[9] F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," Comput. Netw., vol. 47, no. 4, pp. 445–487, 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 Commun., vol. 14, no. 5, pp. 85–91, Oct. 2007.

[11] Federal Aviation Administration, U.S. Department of Transportation. (2015). New Rules for Small Unmanned Aircraft Systems [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 Standard 802.11, 2004.

[13] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11, 2012.

[14] 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. 2486–2491.

[15] M. Sbeiti and C. Wietfeld, "The agony of choice: Behaviour analysis of routing protocols in chain mesh networks," in Proc. Int. Conf. Ad Hoc Netw., 2014, vol. 129, pp. 65–81..