JOURNAL OF AERONAUTICS AND SPACE TECHNOLOGIES
JULY 2016 VOLUME 9 NUMBER 2(13-21)

SECURITY ISSUES IN FLYING AD-HOC NETWORKS (FANETs)

İlker BEKMEZCİ*

Department of Computer Engineering, Aeronautics and Space Technologies Institute, Turkish Air Force Academy, Istanbul, Turkey 34149, i.bekmezci@hho.edu.tr

Eren ŞENTÜRK

Department of Computer Engineering, Aeronautics and Space Technologies Institute, Turkish Air Force Academy, Istanbul, Turkey 34149, erensenturk@thy.com

Tolgahan TÜRKER

Department of Computer Engineering, Aeronautics and Space Technologies Institute, Turkish Air Force Academy, Istanbul, Turkey 34149, tturker@hho.edu.tr

Received: *02nd February 2016,* ***Accepted:*** *13rd April 2016*

ABSTRACT

Technological advancements in Unmanned Aerial Vehicles (UAV) encourage the use of multi-UAV systems in military and civil applications. The most important benefit of the multi-UAV system is to fulfill missions that require collaborative and cooperative behavior which depends on communication between UAVs. Flying Ad-Hoc Network (FANET) is a technique that both solves the coverage range problem between ground station and the UAVs; and supports real time data transfer without any infrastructure. FANET, which can be considered another type of ad-hoc network, holds all security issues of ad-hoc networks. Besides, it might also have new security problems, because it consists of UAVs. In this paper, FANET security limitations and challenges are surveyed. In addition, open research areas are also discussed.
.

Keywords*: ad-hoc networks, FANET, security.*

1. INTRODUCTION

Unmanned Aerial Vehicle (UAV) systems are becoming more popular in both military and civilian applications in the so-called 4D tasks: tasks that are dangerous, dull, dirty, or dumb [1]. Search and rescue operations, border surveillance, target detection, disaster monitoring, managing wildfire, traffic monitoring are some application areas for UAVs [2].

By the help of the technological advancements in electronic and avionic systems, the production of small or mini UAVs is ensured. There are several advantages of smaller UAV systems. The purchase value, as well as maintenance and repair costs of mini UAVs are reduced. In addition, they are built and operated more easily [1]. The radar cross-section is smaller; and they can depart within limited take-off distance. However, small UAVs have more restricted capabilities compared to large UAVs. In order to achieve the missions with mini UAVs formerly conducted by large UAVs, multi-UAV systems are developed.

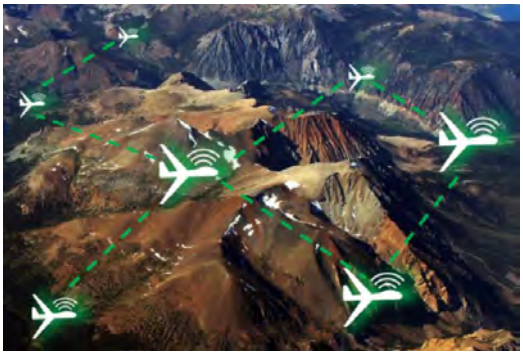


Figure 1. FANET sample structure illustration.

One of the most essential design considerations of multi-UAV systems is communication. Ground and satellite based solutions are offered so as to provide communication among UAVs. However, these solutions have communication range constraints. Obviously, such systems require a communication infrastructure that should be prepared beforehand. This infrastructure-based communication structure is not easy to build especially in disaster and military

missions. One of the most important multi-UAV communication systems, which can transfer data to the base-station independently from communication range and infrastructure in real time, is Flying Ad-Hoc Network Flying Ad-Hoc Network (FANET) [2]. In this paper, the security issues of FANETs are discussed.

FANET is an ad-hoc network structure which is formed solely by UAVs. Hence, it differs from existing ad-hoc networks such as Mobile Ad-Hoc Network (MANET) and Vehicle Ad-Hoc Network (VANET) in terms of design and security issues. First of all, FANET nodes have higher mobility degrees, and it results in more frequent changes in the topology of FANETs. Moreover, the distance between the nodes in FANETs are longer in comparison to the nodes in other ad-hoc networks. For FANETs, the communication range should be longer than in the MANETs and VANETs in order to establish communication links between UAVs. Also, because the nodes in FANETs are physically smaller, the equipment they can carry is limited [2]. The existing ad-hoc security studies can be ineffective or cannot be operated due to the structure of FANET. The FANET characteristics that avoid the existing ad-hoc security issues are provided below.

• Node Movement Autonomy: The nodes in FANET may display instant behaviors in return for a certain event, including the course of action and routing order. Therefore, it may not always be right to make presumptive plans according to the actions or routes of the node [2].

• Power Limitation: Especially for FANETs formed by mini UAVs, electric capacity is very limited. Attacks made on such limited energy sources may cause nodes to deactivate [2].

• Memory and Computation: The memory and computation abilities of the nodes in FANETs are limited. Therefore, there is a possibility of not actualizing cryptology methods requiring high level of memory and computation capacity [2].

• Node Mobility: Nodes forming FANET may change their places in a much shorter time interval [2].

• Node Density: FANET nodes may be far apart in the sky. So, the node density in FANET is much lower in comparison to MANET and VANET [2].

• Localization: It is hard to determine the accurate location of the nodes in FANET because of their high mobility degree. Localization data should be updated in smaller time intervals [2].

There are several studies about ad-hoc networks in the literature [3], [4], [5], [6]. However, the existing security studies and algorithms may become illegitimate for FANET, because it differs from MANET and VANET by its characteristic features. This paper presents a survey about security issues in FANET. The organization of the paper is as follows. In Section II, general ad-hoc network security issues are presented by covering security goals, attacks and solutions. In Section III, security issues in FANET are considered by comparing their differences with other ad-hoc networks. Open security issues for FANET are pointed out in Section IV. Finally, the paper is concluded in Section V.

2. GENERAL AD-HOC NETWORK SECURITY ISSUES

It can be decided whether an ad-hoc network is secure or not by depending on the basic security criteria provided below. Even if the system meets all of these criteria, it does not necessarily mean that it is totally secure. However, if the system does not fulfill one of these criteria, then it can be concluded that the system is not secure.

Availability refers to a node being convenient, existing and usable within its life cycle in any time and condition. When a node is attacked, the node should still perform its service without being affected by the attack. An example of such attacks is denial of service [7].

Integrity means not altering a message consciously or unconsciously. Deleting or changing the content of the messages with the purpose of malicious activity breaks the integrity of the system [7].

Confidentiality allows the information to be accessible by only authorized nodes [8]. By this means, the objective is to guarantee the secrecy of the confidential information.

Authenticity is to guarantee the submission of the real identities of nodes [8]. In cases where there is no structure under guarantee, the attackers may express themselves with other identifications and perform an attack by using these authorizations.

Non-repudiation refers to not denying that the operations were conducted [8]. It may display abnormal behaviors with the intention to cause damage as a result of a node sending erroneous or wrong messages. These abnormalities may also have the intention to interrupt the usability of the network, along with causing congestion within the network. Where such situations are identified, the node causing the problem would ensure not denying that the relevant operations were conducted automatically.

Authorization means giving permission to access resources regarding the identification, following the confirmation process of the identification [9]. Different authorization levels are given to the sources and the nodes. By this means, nodes can conduct

operations within their own authorization levels on the sources with only h the same level of authorization.

Anonymity is to keep the identification information of the nodes private. Also, that information should not be distributed by the nodes. In this manner, the node shares its authorization only with the nodes it wants. This criterion enables hiding the identities of nodes from vicious nodes.

2.1 Attacks on Ad-Hoc Networks

Ad-hoc security attacks have been examined in many studies [10], [11], [12]. These studies show that attacks may aim to seize control, or merely leak sensitive data or sabotage the mission by creating anomaly on the network [13]. Where the control of a network is taken by its opponents within an attack, it is clear that the network is already invaded. However, attacks other than these are hardly detected due to the difficulties in distinguishing the behaviors of infected networks from casual networks. In this part, we focused on known security issues.

2.1.1 Eavesdropping

Eavesdropping is much easier in a wireless environment than in a wired environment [14], [15], [16]. For a wired medium, there is an obligation to reach the cable itself. However, there is no such requirement for a wireless environment. It is enough to be inside the environment where the communication is conducted. Even if the data is encrypted in wireless communication, it may be listened by a malicious node. There is a possibility of guessing the encryption by making an analysis through encrypted packages obtained from the communication in the wireless medium. The only purpose of this type of attacks is to listen in, and no change is made within the content of the package. Therefore, it is difficult to understand that an attack is performed.

2.1.2 Modification and Fabrication

Attack Using Modification Attacks: While protocols such as AODV transmit a package from one node to another, they increase its sequence number. An attacker node may notify that it has reached the target by showing its sequence number lower [17]. Thus, it may try to reach the target by a route set through the attacker, instead of the ordinary route. Hop Count:

Hop Count means the number of intermediate nodes through which a packet should pass between the source and the destination. It could reach the information regarding how many nodes a packet passed to the target by looking at hop count. An attacker node might change this information with the purpose of spoofing or might even initialize it to zero. If the optimum path can be found through hop count, it may be unreachable as the value changes. Thus, the connection would be made through a wrong path [18].

Source Node Modification: Routing embed the route which the package tracks in case an attacker node changes this value [17]. By randomly changing the directions of these packages, it forms an obstacle regarding the package reaching the target [17]. Because it does not change the route of the packages constantly, the detection of this attack is more difficult.

Spoofing Attack: Spoofing attack is an attack by showing its own IP or MAC address as a different IP or MAC address. It does not necessarily have to be through an IP or MAC address but also could be conducted by changing another identifier. As a result, if an identifier based process is conducted, a weakness may be created.

Attack Using Fabrication: It is a type of attack conducted by sending false routing message. Thus, by sending false messages, the attacker may reveal a valid route as if it is invalid, or contrarily, it may reveal an invalid route as if it is valid.

Rushing Attacks: Once the nodes receive a discovery package, they can neglect the second one for the purpose of route optimization. An attacker node can send the discovery messages faster and in a much more offensive manner than the other nodes. If it manages to be the first who sends the discovery packages, the receiver nodes cannot serve their function properly to the nodes other than the attacker node [18]. In order to realize and continue this attack, the attacker nodes should send the discovery messages before allowing other nodes; and this would cause a network overhead.

Wormhole Attacks: Wormhole is an attack that mainly tries to leak information by creating a tunnel between nodes that consist of at least one malicious node. Malicious nodes can relay a copy of packets to outside the network in order to analyze or simply drop them to cause anomalies [19]. Symptoms of wormholes are not apparent due to the mobile nature of ad-hoc networks. Slowness may be caused either by a wormhole or by bad environmental conditions. Making a distinction between them is difficult. It is also known as the tunnelling attack [20].

Gray Hole Attack: If the attacker node somehow manages to get involved in the route, it can drop the received package [21]. Since this case is interpreted as the target node is not reachable at that moment, it is difficult to determine the attacker node. Furthermore, the attacker node may perform false forwarding in

order to cause a disorder or may ensure the non-arrival of the data by removing a node from the routing table.

2.1.3 Selfishness

Performing data transmission is not the fundamental duty of the nodes forming MANET. It means that they might not conduct their routing or package transmission duties as a priority within their schedule. If one of the nodes is conducting the data process very slowly or late, this fact may affect all the transfer process passing through that node and cause a slowing down. Furthermore, even if this is not a type of attack, it would interrupt the operation of the system [3].

2.2 Existing Countermeasures for Ad-hoc Network Security Attack

Security mechanisms can be classified as preventive and reactive. While the preventive approach aims to prevent security breach by using methods such as cryptology, reactive approach aims to determine the security breach itself. Intrusion detection system can be given as an example. It is indicated that the usage of both mechanisms together should make the network securer [8]. Ad-hoc network security countermeasures that are surveyed in this paper are presented for different network layers. [8].

2.2.1 Physical Layer

As there is no electrical conductor for providing data communication within ad-hoc nodes, the signals could be sniffed out easily. The scope that could be sniffed might be narrowed by the usage of directional antennas [22] and by the usage of different modulation techniques. Eavesdroppers seeking to analyze the data could encounter difficulties. Moreover, jamming attacks could be performed in order to disturb communication. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are suggested against such attacks [23]. Thereafter, Uncoordinated Frequency Hopping (UFH) and Uncoordinated DSSS, which remove re-shared key dependency that exist within FHSS and DSSS are proposed [24]. Frequency Hopping with Uncoordinated Seed Disclosure (USD-FH), based on key exchange, is proposed by Liu et al., which is more efficient than the previous studies [24]. Randomized Differential DSSS is developed by Liu et al. without the need of a shared key [25]. Moreover, jamming and anti-jamming issues that are aware of the movements of the nodes are proposed by He et al. [26].

2.2.2 Link Layer

Link layer is responsible for media access, error control and flow control. The selfish usage of the media would harm the network as much as Denial of Service (DOS) [26]. A mechanism that detects and prevents the selfishness is published by Cardenas et al. [27]. Ren et al. have proposed a power efficient Link-Layer Security Protocol (LLSP), which conducts authentication and message integrity check [28].

2.2.3 Network Layer

Wormhole attacks:
The detection metrics of wormhole attacks in ad-hoc networks are indicated by Mahajn et al. as follows [29]:

Strength: Tries to attract the network traffic upon itself. The fact that the same node exists in many of the end to end paths strengthens the possibility of a wormhole [29].

Path Length: If there is a difference between the length of the advertised path and the valid path, the possibility of a wormhole is strengthened [29].

Attraction: If there is a new shorter path that occurred on an existing end to end path length, the cause of this could be a wormhole attack [29].

Robustness: This means that the wormhole persists even when a structure change occurs in a network [29]. If the same node persists inside the path following topological changes, the reason of this might be a wormhole.

Prevention: Without the need of a special hardware named Wormhole Attack Prevention (WAP), Choi et al. developed a method that ensures prevention and identifies the wormhole in the discovery phase [30].

Additionally, Nayak et al. presented methods that conduct detection and prevention without the need of location, specific hardware and clock synchronization [31].

Black hole attacks: A defence mechanism against multiple black hole nodes is proposed by Sen et al. [32]. A solution that detects the malicious node for ad-hoc On-demand Distance Vector (AODV), which is a network routing protocol, is proposed [33]. Additionally, an approach based on trust on neighbour nodes is developed [34]. Moreover, it is stated that security-aware ad-hoc routing protocol (SAR) based on demand protocol could be used in preventing black hole attacks [8].

Impersonation and repudiations: Authentication mechanism is needed for preventing impersonation and repudiation. Authenticated Routing for Ad-Hoc Networks (ARAN) that provides an authentication service prevents impersonation and repudiation by ensuring predetermined certificates and end-to-end authentication [8].

Modification attacks: They are the countermeasures which aim to protect the integrity of the package against attacks that change the contents of the package such as the sequence number of the package. Secure efficient distance vector routing for mobile wireless ad-hoc networks (SEAD) protocol, which tries to prevent modification by using a one-way hash chain, can be given as an example [8].

2.2.4 Transport Layer

Attacks that are known against transport layer are SYN flooding [35] and session hijacking attacks [36]. The fact that Transmission Control Protocol (TCP) is connection oriented makes it vulnerable against SYN flooding attacks. As TCP is not directly used in ad-hoc networks, new protocols like TCP are invented. However, the security issue is ignored during their design. New protocol arrangements considering the needs and security requirements of ad-hoc networks is an open-ended issue [8].

2.2.5 Application Layer

Application layer provides services such as firewall access control, user authentication, packet filtering and logging by using traditional methods. However, as there is a lack of structure within ad-hoc networks, applying firewall is not as useful as traditional methods.

3. FANET COMMUNICATION SECURITY

Communication is the key component for UAV applications. Besides the reliable and efficient data transmission problems in UAV communication technology, security issues also have been taken into consideration against malicious acts on the channel. Therefore, the interest in UAV communication security has increased with the recognition of security vulnerabilities of UAV communication subsystems and its potential severity of consequences [37]. In this sense, a lot of research on UAV communication security issues has been conducted in recent years. In this section, the important studies on UAV communication security is presented.

One of the most comprehensive studies on communication security for multi-UAV systems, more related with the FANET concept, is conducted by Phillips et al.. in connection with an efficient group key management. In [38], a multicast secure group communication architecture (Hubenko, et al.) for LEO satellite networks in the global information grid [39] is analyzed to determine if it can be adapted to heterogeneous UAV swarm applications, and to provide a secure and efficient communication. The main focus of the study is to provide efficient and scalable architecture for group re-keying, which is needed for encrypting and decrypting group communication. It is concluded that Hubenko study can be used as a secure group communication architecture for UAV swarms with performance improvements in terms of group key management compared to the other widely used security architectures, namely baseline and cluster.

Another study on UAV communication security is conducted by Rudinskas et al. Potential problems based on the communication radio, possible threats to the radio connection system, and corresponding solutions for secure communication are discussed in [40].

In [41], MILS (Multiple Independent Levels of Security) is analyzed for UAV system design needs in terms of information and communication security. The main focus in MILS is to take the advantage of partitioned architecture to obtain assurance levels.

Kim, et al. have identified the security vulnerabilities of current autopilot systems in UAVs in three groups: Hardware attacks, Wireless attacks, and Sensor attacks, and Sensor attacks, and analyzed the behaviour of the system after an attack occurs in [42]. A cyber-secure architecture for autopilot system based on a cyber-security monitoring component Supervisor is proposed, which is responsible for detection and isolation of malicious activities within the autopilot system. The simulation results have shown the proposed cyber-secure architecture makes the overall system more robust against cyber-attacks.

A study on the impacts of falsified GPS signals on an autonomous UAV is conducted by Kerns, et al. The requirements for the capture of UAVs navigation system are discussed by providing results from the practical tests against many commercial GPS receivers. Repeatedly performed attacks at different power advantage factors show that an attacker may manage to capture the target UAV up to 50 m position and 10 m/s velocity estimation error [43].

In another study, spatially secure group communication (SSGC) problem is investigated for multiple unmanned autonomous vehicles to analyze communication impacts on group dynamics and spatial communication security [44]. As a distributed solution, a UAV formation approach, which is based on the modification of wireless communication parameters for each group member, is proposed. The feasibility of the proposed solution is demonstrated within the context of a potential military scenario.

Bhattacharya, et al. have analyzed jamming attacks on multi- UAV communication systems as a zero-sum pursuitevasion game. In order to obtain optimum strategy for UAVs in the existence of a mobile

jammer, a game theory based approach is developed in [45]. In a similar context, in [46], the jamming problem is turned into a resource allocation problem with power limitations of each UAV, and a general two-player game concept of differential game theory is modified to a twoteam multiplayer game.

Another secure communication scheme for FANETs is investigated by Chaumette, et al. In [47], deployment of an embedded smart card is proposed to provide required security functionalities based on the authors previous study on distributed identity management for MANETs [47]. Low level radio security is presented as to be managed by using dedicated hardware components to deal with proper choice of radio frequency. In addition, software level security is dealt with by embedding smart cards to be able to have cryptographic functionalities in order to achieve secure dynamic group management. In a similar hardware-based solution context, Akram, et al. have characterized the security requirements of autonomous UAV swarm applications in the presence of strong adversary scenarios. Also, a theoretical solution Active Radio Frequency Smart Secure Device (ARFSSD) is proposed as an embedded secure element (SE) based on security architecture in order to satisfy defined requirements. A comparison of SEs which can be deployed on unmanned vehicles is made. In addition, the proposed solution (ARFSSD) is formed by utilizing the best features of Wireless Sensor Node, Trusted Platform Module, Smart Card, and Active RFID, which are evaluated as candidate SEs [48].

A secure 3D positioning approach based on multilateration algorithm and Received Signal Strength Indicator (RSSI) for UAV swarms is proposed in [49]. The purpose of the proposed verification method is to detect false/fake positions adopted by a UAV in the swarm. The results show the feasibility of the proposed architecture for secure positioning.

Another important issue is test beds and simulation environments for communication security of multi-UAV systems. Javaid, et al. have presented a detailed review of recent advances in UAV security test beds and a performance analysis of UAVSim test bed for single and multi-UAV communication security by using DDoS attack and jamming attack, respectively [50].

4. OPEN RESEARCH ISSUES

There are certain differences between FANET and existing ad-hoc networks. The main reason is that FANET nodes are composed entirely of UAVs which lead to frequent changes in topology because of their high mobility degrees. There are also other factors such as operation environment, node density, localization, power consumption, etc. [2]. While some of these factors may bring out new vulnerabilities, others may contribute to eliminating some existing security flaws. Within the FANET, an analysis of existing defense mechanisms against security threats in MANETs and VANETs can be considered one of the open research areas. In this section, some open research issues about FANET security are investigated.

4.1 Communication Issues for FANET

A UAV mostly operates in line of sight environment, so it is more likely to eavesdrop than the other ad-hoc networks. The usage of directional antennas instead of omni-directional antennas in FANET applications can make the attacks more difficult. Using directional antennas provides data transmission through the desired direction and reduces the probability of eavesdropping and jamming [51]. Moreover, directional antennas can be used to protect the system against wormhole attacks. Directional antennas also obtain longer transmission ranges [52]. As UAVs operate in a quick and autonomous manner, location of UAVs changes often, and this causes UAVs to be out of the range of the directional antenna. For this reason, adaptive MAC protocols are implemented for UAVs [52]. Another important issue that affects the performance of FANET is awareness of the exact location of neighbour nodes. Location Oriented Directional MAC Protocol (LODMAC) for FANETs is implemented as a remedy for estimating the location of neighbour UAVs [22].

4.2 Free Space Optical Communication

One of the most promising technologies for FANET communication security is free space optical communication systems. Besides its extremely high communication speed, it also promises higher communication security levels [53]. Free space optical communication systems have narrow optical beam paths, which are inaccessible unless viewing directly into the transmitter path. As free space optical communication transmits more data by spreading its signal into smaller area compared to the directional antennas, the possibility of eavesdropping is reduced. However, free space optical communication can be affected by the weather. Moreover, point acquisition problem may occur due to point to point communication. Most of the research on this topic is about ground to UAV communication structure [54]. Point acquisition may be more difficult in FANET because of its UAV to UAV communication structure. Fortunately, there are some demonstrations that show free space optical communication between aircraft is possible, and that it can also be used for FANETs [55]. Especially Vialight Communication Company asserts miniaturized laser communication terminals

that enable a reliable, stealth and point to point communication.

4.3 UAV Platform Constraints

Physically smaller UAVs are preferred in FANET applications. It means that each UAV has limited capacity in FANET. So, they can be easily stolen. This is a serious threat especially for military applications. The information it carries and the encrypting methods should not be acquired by the opponents. Because of the size and cost constraints of the UAVs, complex hardware systems cannot be mounted. Moreover, the technologies that we do not want to be captured by opponents might not be employed in FANET due to the possibility of hijacking. In such cases, applying existing technologies to FANET can be a more suitable approach. By hijacking the UAV, opponents can study an attack to the following generation of the same UAV with the reverse engineering concept. This state may cause the malfunction of the algorithms or a leak of information. During the implementation of the FANET algorithms, it should be considered that UAVs can be hijacked and consequently the algorithms used in them may be brought into open.

4.4 New Node Addition

In many applications, node density is lower in FANET than in MANET or VANET; and usually, relay nodes are needed for data transmission from UAV to ground base. The reliability of these nodes directly affects the network security. In case one of these nodes fails, the network connection may become unavailable. Sometimes, it may be necessary to add new UAVs in place of unavailable nodes. In such cases, it is necessary to identify the new node before performing an operation.

4.5 Independency from Ground Station

One of the most important features of FANET is that it operates without any ground station. However, most of the available security architectures are dependent on the existence of ground stations. Adapting ground solution based approaches successfully, and fulfilling the security needs of ad-hoc networks such as MANET and VANET by especially considering the highly dynamic characteristic of FANET is an open-ended research area.

5. CONCLUSION

One of the most important features of FANET is that it operates without any ground station. However, most of the available security architectures are dependent on the existence of ground stations. Adapting ground solution based approaches successfully, and fulfilling the security needs of ad-hoc networks such as MANET and VANET by especially considering the highly dynamic characteristic of FANET is an open-ended research area.

6. REFERENCES

[1] O. K. Sahingoz, “Networking models in flying ad-hoc networks (fanets): Concepts and challenges,” Journal of Intelligent & Robotic Systems, vol. 74, no. 1-2, pp. 513–527, 2014.

[2] I. Bekmezci, O. K. Sahingoz, and S¸. Temel, “Flying ad-hoc networks (fanets): A survey,” Ad Hoc Networks, vol. 11, no. 3, pp. 1254–1270, 2013].

[3] D. Djenouri, L. Khelladi, and N. Badache, “A survey of security issues in mobile ad hoc networks,” IEEE communications surveys, vol. 7, no. 4, pp. 2–28, 2005.

[4] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, “A survey of routing attacks in mobile ad hoc networks,” Wireless communications, IEEE, vol. 14, no. 5, pp. 85–91, 2007.

[5] L. Abusalah, A. Khokhar, and M. Guizani, “A survey of secure mobile ad hoc routing protocols,” Communications Surveys & Tutorials, IEEE, vol. 10, no. 4, pp. 78–93, 2008.

[6] P. M. Jawandhiya, M. M. Ghonge, M. Ali, and J. Deshpande, “A survey of mobile ad hoc network attacks,” International Journal of Engineering Science and Technology, vol. 2, no. 9, pp. 4063–4071, 2010.

[7] L. Zhou and Z. J. Haas, “Securing ad hoc networks,” Network, IEEE, vol. 13, no. 6, pp. 24–30, 1999.

[8] B. Wu, J. Chen, J. Wu, and M. Cardei, “A survey of attacks and countermeasures in mobile ad hoc networks,” in Wireless Network Security, pp. 103–135, Springer, 2007.

[9] V. Atluri and W.-k. Huang, “An authorization model for workflows,” in Computer Security-ESORICS 96, pp. 44–64, Springer, 1996.

[10] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” Wireless Communications, IEEE, vol. 11, no. 1, pp. 38–47, 2004.

[11] M. Raya and J.-P. Hubaux, “The security of vehicular ad hoc networks,” in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pp. 11–21, ACM, 2005.

[12] R. Akbani, T. Korkmaz, and G. Raju, “Mobile ad-hoc networks security,” in Recent Advances in Computer Science and Information Engineering, pp.

659–666, Springer, 2012.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255–265, ACM, 2000.

[14] Y. Zou, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances and future trends," arXiv preprint arXiv:1505.07919, 2015.

[15] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," Communications Surveys & Tutorials, IEEE, vol. 15, no. 1, pp. 446–471, 2013.

[16] A. Mukherjee, S. A. Fakoorian, J. Huang, A. L. Swindlehurst, et al., "Principles of physical layer security in multiuser wireless networks: A survey," Communications Surveys & Tutorials, IEEE, vol. 16, no. 3, pp. 1550–1573, 2014.

[17] P. Ning and K. Sun, "How to misuse aodv: a case study of insider attacks against mobile ad-hoc routing protocols," Ad Hoc Networks, vol. 3, no. 6, pp. 795–819, 2005.

[18] H. L. Nguyen and U. T. Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks," Ad Hoc Networks, vol. 6, no. 1, pp. 32–46, 2008.

[19] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," Selected Areas in Communications, IEEE Journal on, vol. 24, no. 2, pp. 370–380, 2006.

[20] S. Shrivastava and S. Jain, "A brief introduction of different type of security attacks found in mobile ad-hoc network," International Journal of Computer Science & Engineering Technology (IJCSET), vol. 4, no. 3, 2013.

[21] A. Dorri, S. R. Kamel, and E. Kheirkhah, "Security challenges in mobile ad hoc networks: a survey," arXiv preprint arXiv:1503.03233, 2015.

[22] S. Temel and I. Bekmezci, "Lodmac: Location oriented directional {MAC} protocol for {FANETs}," Computer Networks, vol. 83, pp. 76 – 84, 2015.

[23] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," Communications Surveys & Tutorials, IEEE, vol. 11, no. 4, pp. 42–56, 2009.

[24] A. Liu, P. Ning, H. Dai, and Y. Liu, "Usd-fh: Jamming-resistant wireless communication using frequency hopping with uncoordinated seed disclosure," in Mobile Adhoc and Sensor Systems (MASS), 2010 IEEE 7th International Conference on, pp. 41–50, IEEE, 2010.

[25] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential dsss: Jamming-resistant wireless broadcast communication," in INFOCOM, 2010 Proceedings IEEE, pp. 1–9, IEEE, 2010.

[26] X. He, H. Dai, and P. Ning, "Dynamic adaptive anti-jamming via controlled mobility," Wireless Communications, IEEE Transactions on, vol. 13, no. 8, pp. 4374–4388, 2014.

[27] A. A. Cardenas, S. Radosavac, and J. S. Baras, "Detection and prevention of mac layer misbehavior in ad hoc networks," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 17–22, ACM, 2004.

[28] J. Ren, T. Li, and D. Aslam, "A power efficient link-layer security protocol (llsp) for wireless sensor networks," in Military Communications Conference, 2005. MILCOM 2005. IEEE, pp. 1002–1007, IEEE, 2005.

[29] V. Mahajan, M. Natu, and A. Sethi, "Analysis of wormhole intrusion attacks in manets," in Military Communications Conference, 2008. MILCOM 2008. IEEE, pp. 1–7, IEEE, 2008.

[30] S. Choi, D.-y. Kim, D.-h. Lee, and J.-i. Jung, "Wap: Wormhole attack prevention algorithm in mobile ad hoc networks," in Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on, pp. 343–348, IEEE, 2008.

[31] P. Nayak, A. Sahay, and Y. Pandey, "Detection and prevention of wormhole attacks in manets using detection packet," International Journal of Scientific & Engineering Research, vol. 4, no. 6, pp. 1216– 1222, 2013.

[32] J. Sen, S. Koilakonda, and A. Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks," in Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on, pp. 338–343, IEEE, 2011.

[33] L. Himral, V. Vig, and N. Chand, "Preventing aodv routing protocol from black hole attack," Lalit Himral et al./International Journal of Engineering Science and Technology (IJEST), vol. 3, no. 5, 2011.

[34] F. Thachil and K. Shet, "A trust based approach for aodv protocol to mitigate black hole attack in manet," in Computing Sciences (ICCS), 2012 International Conference on, pp. 281–285, IEEE, 2012.

[35] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "Dos attacks in mobile ad hoc networks: A survey," in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, pp. 535–541, IEEE, 2012.

[36] K. Sahadevaiah and P. R. PVGD, "Impact of

security attacks on a new security protocol for mobile ad hoc networks," Network Protocols and Algorithms, vol. 3, no. 4, pp. 122–140, 2011.

[37] J. Goppert, W. Liu, A. Shull, V. Sciandra, I. Hwang, and H. Aldridge, "Numerical analysis of cyberattacks on unmanned aerial systems," in AIAA Conference on Infotech@ Aerospace, 2012.

[38] A. N. Phillips, B. E. Mullins, R. A. Raines, and R. O. Baldwin, "A secure group communication architecture for autonomous unmanned aerial vehicles," Security and Communication Networks, vol. 2, no. 1, pp. 55–69, 2009.

[39] V. P. Hubenko Jr, R. Raines, R. O. Baldwin, B. E. Mullins, R. F. Mills, M. R. Grimaila, et al., "Improving satellite multicast security scalability by reducing rekeying requirements," Network, IEEE, vol. 21, no. 4, pp. 51–56, 2007.

[40] D. Rudinskas, Z. Goraj, and J. Stankunas, "Security analysis of uav ¯ radio communication system," Aviation, vol. 13, no. 4, pp. 116–121, 2009.

[41] C. Constantinides and P. Parkinson, "Security challenges in uav development," in Digital Avionics Systems Conference, 2008. DASC 2008. IEEE/AIAA 27th, pp. 1–C, IEEE, 2008.

[42] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber-attack vulnerabilities analysis for unmanned aerial vehicles," Infotech@ Aerospace, 2012.

[43] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via gps spoofing," Journal of Field Robotics, vol. 31, no. 4, pp. 617–636, 2014.

[44] S.-W. Kim and S.-W. Seo, "Cooperative unmanned autonomous vehicle control for spatially secure group communications," Selected Areas in Communications, IEEE Journal on, vol. 30, no. 5, pp. 870–882, 2012.

[45] S. Bhattacharya and T. Basar, "Game-theoretic analysis of an aerial jamming attack on a uav communication network," in American Control Conference (ACC), 2010, pp. 818–823, IEEE, 2010.

[46] S. Bhattacharya and T. Bas¸ar, "Secure communication for mobile agents in an adversarial environment," in Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on, pp. 1–8, IEEE, 2011.

[47] S. Chaumette, R. Laplace, C. Mazel, and A. Godin, "Secure cooperative ad hoc applications within uav fleets position paper," in Military Communications Conference, 2009. MILCOM 2009. IEEE, pp. 1–7, IEEE, 2009.

[48] R. N. Akram, P.-F. Bonnefoi, S. Chaumette, K. Markantonakis, and D. Sauveron, "Improving security of autonomous uavs fleets by using new specific embedded secure elements a position paper,"

[49] R. S. Yokoyama, B. Y. L. Kimura, and E. dos Santos Moreira, "An architecture for secure positioning in a uav swarm using rssi-based distance estimation," ACM SIGAPP Applied Computing Review, vol. 14, no. 2, pp. 36–44, 2014.

[50] A. Y. Javaid, W. Sun, and M. Alam, "Single and multiple uav cyberattack simulation and performance evaluation," EAI Endorsed Transactions on Scalable Information Systems, vol. 15, 2 2015.

[51] Q. Wang, H.-N. Dai, and Q. Zhao, "Eavesdropping security in wireless ad hoc networks with directional antennas," in Wireless and Optical Communication Conference (WOCC), 2013 22nd, pp. 687–692, IEEE, 2013.

[52] A. I. Alshbatat and L. Dong, "Adaptive mac protocol for uav communication networks using directional antennas," in Networking, Sensing and Control (ICNSC), 2010 International Conference on, pp. 598–603, IEEE, 2010.

[53] S. M. Navidpour, M. Uysal, and M. Kavehrad, "Ber performance of free-space optical transmission with spatial diversity," Wireless Communications, IEEE Transactions on, vol. 6, no. 8, pp. 2813–2819, 2007.

[54] A. Carrasco-Casado, R. Vergaz, and J. M. S. Pena, "Design and early development of a uav terminal and a ground station for laser communications," in SPIE Security+ Defence, pp. 81840E–81840E, International Society for Optics and Photonics, 2011.

[55] M. J. Northcott, A. McClaren, J. Graves, J. Phillips, D. Driver, D. Abelson, D. W. Young, J. E. Sluz, J. C. Juarez, M. B. Airola, et al., "Long distance laser communications demonstration," in Defense and Security Symposium, pp. 65780S–65780S, International Society for Optics and Photonics, 2007.

[56] S. A. H. Seno, R. Budiarto, and T.-C. Wan, "A secure mobile ad hoc network based on distributed certificate authority," Arabian Journal for Science and Engineering, vol. 36, no. 2, pp. 245–257, 2011.