Detection of Fabricated CTS Packet Attacks in Wireless LANs

Xiaocheng Zou and Jing Deng

Department of Computer Science
University of North Carolina at Greensboro
Greensboro, NC 27412, USA
{x_zou,jing.deng}@uncg.edu

Abstract. IEEE 802.11 standard employs the RTS/CTS handshake procedure to avoid transmission collision and to improve network throughput. However, such an exchange may become a system vulnerability when malicious nodes send fabricated control messages such as CTS to make false claims of channel reservation. To the best of our knowledge, there exists no systematic detection technique for such fabricated control messages. In this paper, we investigate the adverse effects of such attacks on channel throughput and delivery ratio. In order to mitigate these effects, we propose an approach to detect the fabricated messages. With the help of two-hop neighborhood information, our technique enables jamming detection and allows the targeted node to send a message, which instructs neighboring nodes to ignore the fabricated control message. We perform ns-2 simulations to evaluate the benefit of our scheme.

Keywords: WLAN, Fabricated Control Message, CTS, NAV, Detection.

1 Introduction

IEEE 802.11 wireless LAN (WLAN) standard protocol was designed twenty years ago. Nowadays, this standard [1] is hugely popular in civilian, industrial and military networks. However, the inherent assumption of cooperative users can lead to critical confidentiality and trustworthiness issues, even though wireless network security has been the focus of many research [14, 19, 21].

One technique in IEEE 802.11 standard protocol is distribution coordinating function (DCF), which coordinates medium access for contending nodes. DCF is in fact the carrier sense multiple access with collision avoidance (CSMA/CA) schema which employs RTS/CTS mechanism to combat the hidden/exposed terminal problems. In this scheme, communication goes through a sequence of control/data packet dialogues: Request-To-Send (RTS) packet, Clear-To-Send (CTS) packet, Data (DATA) packet, and Acknowledgment (ACK) packet. DCF allows different nodes in the network to have fair shares of the medium usage.

In order to avoid collisions by packet transmissions from different nodes at various locations, a special field termed Network Allocation Vector (NAV) is included in RTS, CTS, and ACK packets. After receiving the NAV values on these

X. Zhang and D. Qiao (Eds.): QShine 2010, LNICST 74, pp. 105–115, 2011.

control packets, nodes can only use the channel after the NAV timer expired. While this technique works well in allowing nodes to reserve the channel, it also opens the door to malicious attackers or selfish nodes in the network to gain unfair access or prohibit other nodes from accessing the channel.

Researchers have identified several weaknesses that might be exploited by an attacker or a selfish user in the network. For example, a selfish node may choose a small interval time in the back-off procedure [9] or delaying SIFS (Short Inter Frame Spacing) interval time instead of DIFS (Distributed Inter Frame Spacing) between the process of exchanging frames [12]. This would always give the attacker itself a better chance of successful channel reservation. Similarly, it may also achieve the same goal by sending out fabricated control packets to interfere with other nodes . This is sometimes termed *intelligent jamming* [6, 8], as compared to physical jamming [17].

Compared to jamming detection [15, 18] at the physical layer, detection of intelligent jamming is more challenging. Such jammings consume less energy for the attacker while achieving a similar result - denying all other nodes' access to the channel. Due to the lack of proper data-link layer authentication techniques, any node in network could send out control packets such as RTS, CTS, and ACK. With these packets, it could dominate the channel by assigning an arbitrarily large value of NAV. Fabricated RTS attacks can be detected as nodes can sense the status of the channel for the data packet transmission with a longer carrier sensing range, or lower sensing threshold [20]. Fabricated CTS or ACK attacks are more subtle. Among others, one difficulty of detecting such attacks is that these control packets do not carry the packet sender's ID [1].

In this paper, we investigate the CTS jamming attacks and propose our solution to detect these attacks. Our assumption is that a malicious node broadcasts fabricated CTS frame specifying a certain amount of NAV duration time. We further assume that attackers cannot fake the source address of any message that they send out, with a radio-signal fingerprinting technique employed by the honest nodes. On the other hand, they can change the targeting address on the fabricated CTS messages at will. Neighbors of the malicious node are forced to be quiet for this period of time. This strategy could significantly reduce network throughput and diminish network's capacity to perform expected functions. Furthermore, we study the impact of an intelligent malicious node that can adapt to our detection technique by randomly alternating the targeting address in the CTS packets.

We design a schema called address inspection schema (AIS) to detect these attack behaviors. Our main idea is to compare the destination field on the CTS frame with the neighborhood information. If the address does not belong to the two-hop neighborhood set, then the control packet will be labeled as fabricated immediately. Otherwise, there must exist one node in the neighborhood with an ID the same as the destination field and may have sent out an RTS packet. If this node had not sent out an RTS request, it should notify other nodes to ignore the CTS message. Our technique requires some extra information: the two-hop neighborhood information that can be carried on the periodic HELLO messages.

Our paper is organized as follows: Section 2 discusses recent related works. In Section 3, our scheme is explained in detail. Simulation-based performance evaluation is presented in Section 4. In Section 5, we summarize our work and discuss future works.

2 Related Work

Security issues in wireless networks have received considerable attentions from research community in recent years. In [16], Wood and Stankovic identified vulnerabilities at each of the layers between physical layer and transport layer due to different kinds of Denial-of-Service (DoS) attacks. Due to nature of wireless communication, openness, and sharing of physical medium, it is relatively easy for malicious nodes in the network to launch jamming radio signal to disrupt normal operation of network. Xu et al. [17] examined the radio interference attack problem and categorized four jamming attack models: constant jammer, deceptive jammer, random jammer, and reactive jammer. They further designed two schemes to detect jamming attacks by employing empirical methods based on signal strength.

At MAC layer, the randomness of random access protocols (such as IEEE 802.11 medium access control) allows misbehaving or malicious nodes to gain priority to access the shared medium after deviating their behavior from normal operation [2, 7, 13]. In Raya et al.'s paper [12], they found that greedy nodes making a slight modification to some parameters defined in 802.11 standard protocol could substantially increase the chance of channel occupation. The following two categories were classified: one is greedy nodes sending out selectively scrambled frames to increase victim's contention window, which gives rise to collision occurrence on victim's side who is supposed to received RTS, CTS, and ACK packets; the other is nodes manipulating protocol parameters to increase bandwidth share by transmitting after SIFS instead of DIFS, assigning large value to NAV, and reducing back-off time. A detection mechanism was designed but its effectiveness could deteriorate if its existence is known to the attacker.

Radosavac et al. [9, 10] concentrated security issues on malicious nodes choosing not to comply to standard protocol by selecting small back-off interval in order to obtain more shares of the channel over honest and normal nodes. Through modeling observation of sequence measurements of back-off interval used by malicious node, they adopt minimax robust detection approach with objective to optimize performance for the worst-case situations. Furthermore, they presented a method to decrease the number of required samples in the minimax robust detection approach. Therefore, observing node could arrive at a decision as soon as possible. Unfortunately, these techniques only work for back-off interval maneuvering attacks.

Assigning large value to Network Allocation Vector (NAV) is another way that a malicious node could use to lower channel utilization. As pointed out in Bellardo and Savage's paper [3], attackers could fabricate certain control packets with large value in duration field in order to reserve the channel for a long period of time. This is because normal nodes who received such control packets would have to update their NAV variable and be quiet. They proposed to place a limit on the duration field in order to mitigate the effect of such attacks. This would work for attacks of changing the NAV values on RTS and ACK frames, but not for CTS frame. This is because the hidden nodes from the data sender could not overhear the RTS frame and have no way of limiting the values for NAV on a subsequent CTS frame. In this paper, we present an approach to allow even hidden nodes to distinguish unsolicited CTS frames from legitimate ones, with the help of two-hop neighbor information.

Other solutions have also been investigated. Ray et al. [11] explained the false blocking problem from RTS/CTS mechanism in IEEE 802.11, which would not only propagate to entire network, but also give rise to deadlock situations. To solve this, they presented RTS validation approach to allow nodes receiving RTS packets defer a small period of time ending at the time when corresponding DATA packet is supposed to begin, instead of deferring the longer period specified in the duration field. Zhang et al. [20] studied jamming ACK attack, which has two advantages to attacker, low energy consumption for attacker and great damage to victim. The size of ACK packet is short and it consumes small amount of energy. An Extend NAV schema (ENAV) scheme was proposed to extend the ACK transmission window from T_{ACK} to $R \cdot T_{ACK}$, which reduces the chance of collision between normal ACK packet and fabricated ACK packet. Chen et al. [4] proposed NAV validation approach to check that a subsequent packet will be received at certain time. For instance, DATA frame should be received within *RTS_DATAHEAD_Time* after RTS. Similarly, ACK frame is supposed to be received within *CTS_ACK_Time* after CTS packet. However, malicious nodes switching between CTS and ACK packet could avoid detection.

3 Jamming Detection

In this section, we introduce a countermeasure called address inspection schema (AIS) to mitigate the effect of CTS jamming attack.

First of all, we declare several notations that will be used throughout this work. We define N_k as the neighbor set of node k. Furthermore, we use N'_k to represent the two-hop neighbor set of node k, which can be computed by the union of neighbor sets of node k's neighbor nodes. So, $N'_k = \bigcup_{j \in N_k} N_j$.

The main idea of our AIS technique is to check the targeting address carried on the CTS packets. With the help of two-hop neighborhood information, nodes can decide whether the targeting address of a CTS packet is legitimate. This is because, except in dynamic networks, all overheard CTS packets should have targeting addresses that belong to the two-hop neighborhood set. This is true for each of the neighbors of the CTS packet sender. The decision-making procedure for each node receiving or overhearing CTS packet has the following phases:

Prerequisite phase: Node k sends out HELLO message carrying N_k to all its neighbors so that other nodes can obtain their neighborhood information. This phase should be performed periodically. It is important to ensure the freshness of N'_k.

Inspection phase: Node k inspects targeting address specified in the RA (Receiver Address) field of CTS packet. One of the following scenarios may arise

- **I1:** the targeting address is k and node k has sent an RTS packet. The CTS packet is obviously legitimate. Node k proceeds with the normal operation;
- **I2:** the targeting address is k and node k has not sent an RTS packet. The CTS packet is obviously illegitimate. Node k proceeds with the Clearance phase below;
- **I3:** the targeting address is not k and it belongs to the set N'_k. The CTS packet could be legitimate. Node k proceeds with the normal operation, i.e., updating NAV;
- **I4:** the targeting address is not k and it does not belong to the set N'_k. The CTS packet is illegitimate. Node k ignores the CTS packet.

Clearance phase: In this phase, node k sends out a control packet, termed Clear Reservation (CR), to instruct neighbor nodes to ignore the channel reservation from previous CTS control packet. All nodes overhearing a CR message should ignore the CTS packet, recover the original NAV value.

In order to be able to recover the original NAV value after fabricated CTS attack detection, nodes overhearing CTS messages should not simply update their NAV values right away. Instead, they should keep a copy of the FCS of the CTS message and record the current NAV value before updating it. When a CR message is overheard, they will use these information to look for NAV value to recover.

The information carried by CR packet includes frame control, identification of previous CTS packet, source address, etc. Frame control field has the same structure as illustrated in IEEE 802.11 specification, except one new value is introduced for subtype field, CCTS, meaning clear previous CTS packet's reservation. The FCS' field is copied from the FCS field in the fabricated CTS packet. This functions as identification for the detected fabricated CTS message. A detailed CR packet format is provided in Table 1.

Table 1. Packet format of the clear reservation control packet

FIELDS	BYTE	REMARKS
frame control	2	control fields
TA	6	source address
FCS'	4	FCS of the suspected CTS packet
FCS	4	FCS of this message

An illustrative example is provided in Fig. 1. Under different attack methods, the neighboring nodes, if not all, will detect such fabricated CTS messages and clear the channel reservation.

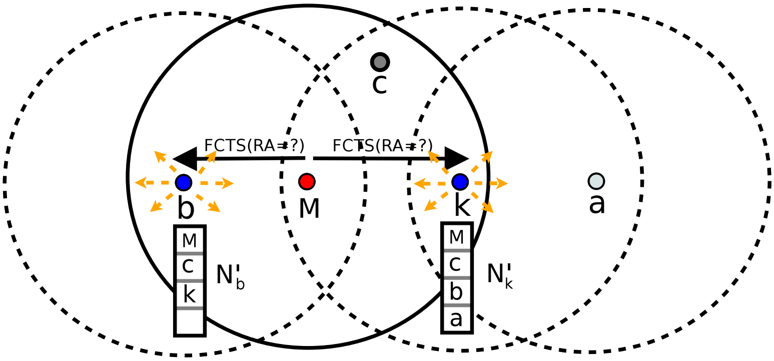

Fig. 1. A scenario illustrating fabricated CTS jamming detection. The network is consisted of five nodes, a, b, c, k, and M. Node M is a malicious node sending out CTS jamming packets randomly. If the targeting address of the fabricated CTS packet from node M is a node outside of this neighborhood, e.g., node x, nodes b, c, and k will detect the jamming and ignore the CTS packet. If node M sends a fabricated CTS targeting at node k, then node k detects it and broadcasts a CR message to notify node c (note that node b is still suffered from the attack). If node M sends a fabricated message to node a, node b detects it and ignores the CTS message (note that node k cannot detect the jamming message).

3.1 Discussions

We have the following discussions regarding to the AIS operation.

Incomplete Detection: As can be seen from the previous discussions, under some attacks, only some neighbors will detect the attack and ignore the fabricated CTS message. Other nodes will still be forced to be silent. This should not have significant impacts on the throughput recovery of the AIS scheme: with some of the nodes in the neighborhood ignoring the fabricated CTS message, they are free to send out channel request or data transmission, occupying the channel instead wasting it for idle. This beats the purpose of the attack.

Communication Overhead: There are two types of additional/revised packets that need to be transmitted: HELLO messages containing each node's neighbor list and the CR message. The HELLO messages are usually broadcast periodically even without the AIS scheme. We only modify the HELLO message to include the neighbor list of the message sender, so that the neighbors can gather information about two-hop neighbors. Note that such information may require some time to obtain.

The CR message will be sent by the node whose ID serves as the targeting address on the fabricated CTS packets. This message is only sent when the node is under attack. As we explained in the Introduction section, we assume that fabricating source address is difficult for attacker (with radio fingerprinting technique in place [5]). Only the node with ID as the targeting address on a suspected CTS message can send a CR message.

4 Performance Evaluation

4.1 Experiment Setup

In order to study the characteristics and evaluate the performance of AIS, we set up simulation experiments using NS2. The wireless transmission range is 250 meters. One node is put into the network serving as the attacker which would periodically send out CTS jamming packets.

We simulated two different types of attacking strategies for the attacker: one targets at non-existing node address, which is termed as “Blind Fabricated CTS” or “Blind FCTS”; the other targets at random node address, which is termed “Focus Fabricated CTS”, or “Focus FCTS”.

Then, we carried out simulation for the following four scenarios.

- **normal:** network under no FCTS attacks and the AIS;
- **Blind FCTS:** network under Blind FCTS attacks but without AIS running;
- **Blind FCTS + AIS:** network under Blind FCTS attacks and AIS is running;
- **Focus FCTS + AIS:** network under Focus FCTS attacks and AIS is running.

Unless specified otherwise, all remaining parameters used in simulations are listed in Table 2. The attack period is the duration for each FCTS packet and the attack interval is the interval between two consecutive attacks.

Table 2. Simulation Parameters

Simulation	25 sec.	Routing Protocol	AODV
Attack Start Time	8th sec.	AIS Start Time	13th sec
Attack Period	6 msec.	Attack Interval	7 msec.
CBR data rate	120Kb	CBR packet size	100 bytes

Our evaluations focus on two major metrics: throughput and delivery ratio. Throughput is defined as the total traffic transmitted in network. Throughput can be considered as the indicator of network functionality. Note that the throughput presented here is the so-called “instant throughput”, which measures the instantaneous throughput, or the number of bits transmitted/received successfully in a unit time. The second major metric that we investigate is delivery ratio, defined as the number of received packets at the receiver divided by the number of transmitted packets. This represents the success ratio of actual transmission.

We first present the results of a pre-assigned network, in which a total of $N = 12$ regular nodes are placed in a field of a 500 × 500 meters. The attacker locates at the center of the network. As Fig. 2 shows, without attacker in network, the data transmission is stable, and overall trend of transmission stays at a horizontal level. However, when the Blind FCTS attack is introduced, throughput drops to

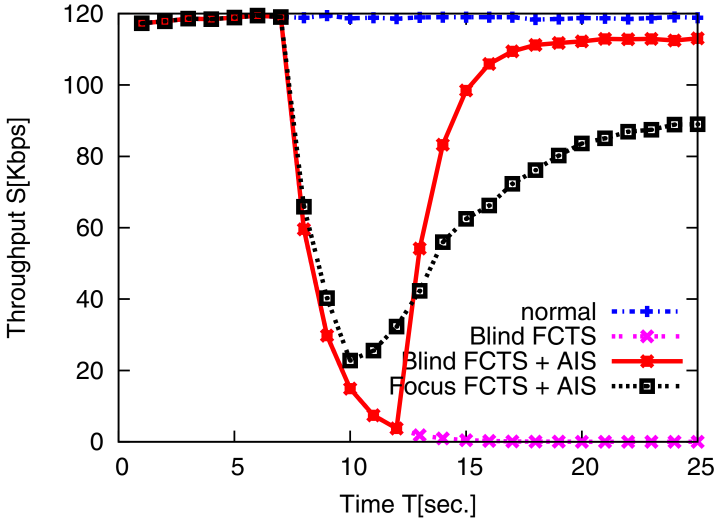

Fig. 2. Throughput performance in normal, Blind FCTS only, Blind FCTS plus AIS and Focus FCTS plus AIS networks. Jamming attack starts at 8th second. AIS kicks in at 13th second. As we can see, AIS helps network to restore most portion of original transmission when network is under attack.

almost 0, starting from the 8th second, which is the attack starting time. This is because the sender is forced to be silent after the Blind FCTS attack.

However, with the help from AIS, victim nodes would ignore illegitimate channel reservation from the attacker, this is demonstrated by two curves in Fig. 2, “Blind FCTS + AIS” and “Focus FCTS + AIS”. After the AIS scheme is activated at 13th second, the throughput curves quickly climb up and approach stable throughput. For Blind FCTS attacks, AIS allows every node to detect such attacks and ignore the corresponding NAV reservations. Based on Fig. 2, the last part of “Blind FCTS + AIS” curve is very close to the curve of the normal network, showing that the network has recovered the throughput to original level.

For Focus FCTS attacks, AIS could only recover a majority of the throughput since attacker alternated targeting address randomly. This could be observed in Fig. 2, i.e., the gap in the stable throughput region between “Focus FCTS + AIS” curve and “Blind FCTS + AIS” curve. The reason for such a gap is the detection failure by the AIS scheme (such as the failed detection by node k when node M sends an FCTS message to node a). In addition, we could observe that the lowest point of “Focus FCTS + AIS” curve is around 20, which is different from that of “Blind FCTS + AIS” scenario. The protection described in IEEE 802.11 standard could explain such a phenomenon: when a node receives unexpected CTS packet targeting to itself, it will discard this packet and is free to use the channel later on.

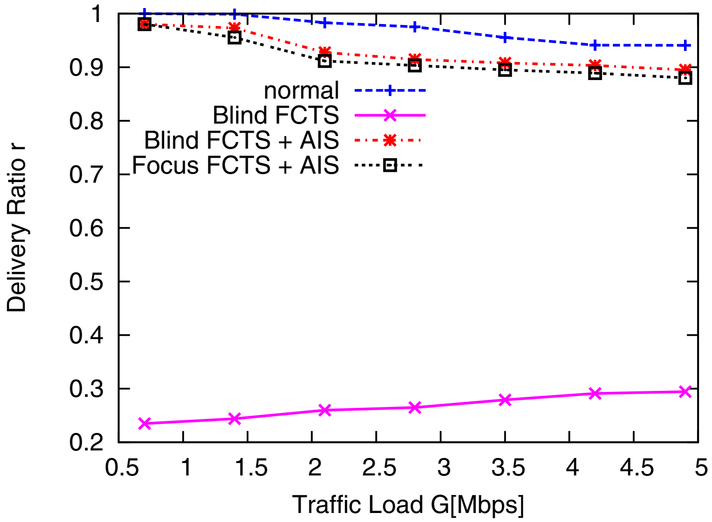

Fig. 3. Delivery ratio comparison in normal, Blind FCTS only, Blind FCTS plus AIS and Focus FCTS plus AIS networks as traffic load increased

We also simulated our scheme in a network where $N = 40$ nodes are placed randomly in a region of 1200×1200. We selected more sender-receiver pairs in order to observe the effect of attack and AIS in a network with higher traffic load.

In Fig. 3, we present delivery ratio results in normal, Blind FCTS only, Blind FCTS plus AIS and Focus FCTS plus AIS networks. The results were obtained through stable conditions, i.e., no dynamic behavior by the attacker or AIS during the observing window. In normal network, overall trend of delivery ratio stays at a high level, and drops slightly at the end, caused by the heavy traffic load. Delivery ratio in Blind FCTS only network is about 0.22 with low traffic load. Seemingly surprisingly, it rises to 0.28 as the traffic load increases. This can actually be explained by the additional pairs of communications, some of which might not be jammed by the attacker.

Networks with AIS running maintain a high delivery ratio, dropping slightly with heavy traffic load. This shows that the use of the AIS technique allows nodes to detect the FCTS attacks and are free to use the channel.

5 Conclusion

In wireless networks, MAC layer has many vulnerabilities and can suffer from different types of attacks. In this work, we have investigated the fabricated CTS attacks to the MAC scheme in wireless LANs. In this attack, an attacker sends fabricated CTS packets with large NAV values to falsely claim the use of the shared channel. We have proposed AIS to mitigate the impact of such jamming attacks. With the help of tow-hop neighborhood information, nodes could distinguish legitimate CTS packets from fabricated ones by observing the targeting address on the CTS packet. When such targeting address falls within the two-hop neighborhood of the attacker, some nodes in the network will be able to detect the attack and ignore the illegitimate claim of channel reservation. Our simulations showed that jamming attack could be easily distinguished, and a significant portion of network throughput can be recovered.

In our future work, we will investigate the jamming attack in mobile networks and evaluate the performance of our proposed scheme in such networks. An approach of delayed action can be used: only after detecting a fabricated CTS message a few times will a node ignore the NAV value from the message. This will provide extra protection for communication of mobile nodes. Theoretical analysis of the performance of our scheme will be performed as well. Furthermore, the overhead of two-hop neighborhood information will be investigated in different networks.

Acknowledgment. We would like to thank Adam Wright, Nihar Kurapati, and Rahul Reddy Maram for their constructive suggestions in the design of our scheme.

References

1. IEEE standard for wireless LAN medium access control and physical layer specifications, p. 802 (November 11, 2007)
2. Awerbuch, B., Curtmola, R., Holmer, D., Nita, C.: Odsbr: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM Transactions on Information and System Security (TISSEC) (January 2008)
3. Bellardo, J., Savage, S.: 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In: USENIX Security Symposium, vol. 12, pp. 2–2 (2003)
4. Chen, D., Deng, J., Varshney, P.K.: Protecting wireless networks against a denial of service attack based on virtual jamming. In: ACM MobiCom 2003 Poster Session, San Diego, CA, USA (September 14-19, 2003)
5. Hall, J.: Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In: Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT), Kranakis, pp. 201–206 (2004)
6. Lazos, L., Poovendran, R., Ritcey, J.A.: Analytic evaluation of target detection in heterogeneous wireless sensor networks. ACM Transactions on Sensor Networks (TOSN) (March 2009)
7. Li, M., Liu, Y.: Rendered path: Range-free localization in anisotropic sensor networks with holes. IEEE/ACM Transactions on Networking, 320–332 (February 2010)
8. Proano, A., Lazos, L.: Selective jamming attacks in wireless networks. In: 2010 IEEE International Conference on Communications (ICC) (May 2010)
9. Radosavac, S., Baras, J.S., Koutsopoulos, I.: A framework for MAC protocol misbehavior detection in wireless networks. In: Workshop on Wireless Security, pp. 33–42 (2005)

10. Radosavac, S., Crdenas, A.A., Baras, J.S., Moustakides, G.V.: Detecting IEEE 802.11 MAC layer misbehavior in ad hoc networks: Robust strategies against individual and colluding attackers. Journal of Computer Security 15, 103–128 (2007)
11. Ray, S., Carruthers, J.B., Starobinski, D.: RTS/CTS-induced congestion in ad hoc wireless lans. Ad Hoc Wireless LANs (2003)
12. Raya, M., Hubaux, J.-P., Aad, I.: DOMINO: a system to detect greedy behavior in ieee 802.11 hotspots. In: International Conference on Mobile Systems, Applications and Services, pp. 84–97 (2004)
13. Richa, A., Scheideler, C., Schmid, S., Zhang, J.: A jamming-resistant mac protocol for multi-hop wireless networks. In: Lynch, N.A., Shvartsman, A.A. (eds.) DISC 2010. LNCS, vol. 6343, pp. 179–193. Springer, Heidelberg (2010)
14. Stajano, F., Anderson, R.: The resurrecting duckling: Security issues in ad-hoc wireless networks. Computer 35, 22–26 (2002)
15. Strasser, M., Danev, B., Capkun, S.: Detection of reactive jamming in sensor networks. ACM TOSN (2010)
16. Wood, A.D., Stankovic, J.A.: Denial of service in sensor networks. Computer 35, 54–62 (2002)
17. Xu, W., Trappe, W., Zhang, Y., Wood, T.: The feasibility of launching and detecting jamming attacks in wireless networks. In: International Symposium on Mobile Ad Hoc Networking and Computing, pp. 46–57 (2005)
18. Xuan, Y., Shen, Y., Shin, I., Thai, M.T.: On trigger detection against reactive jamming attacks: A clique-independent set based approach. In: 2009 IEEE 28th International Performance Computing and Communications Conference, IPCCC (December 2009)
19. Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L.: Security in mobile ad hoc networks: challenges and solutions. Wireless Communication 11, 38–47 (2004)
20. Zhang, Z., Wu, J., Deng, J., Qiu, M.: Jamming ACK attack to wireless networks and a mitigation approach. In: Proc. of IEEE Global Telecommunications Conference / Wireless Networking Symposium (GLOBECOM 2008), New Orleans, LA, USA, November 30 - December 4. ECP, vol. 950, pp. 1–5 (2008)
21. Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Wireless Networks 13, 24–30 (2002)