Mobility Patterns: Local Traffic Strategies With Dynamic Effects

A.LAKSHMAN	T.RAJESH	M.SATEESH KUMAR
M.TECH (CSE) STUDENT	ASST.PROFESSOR	HOD OF CSE
AKULA SRIRAMULU	AKULA SRIRAMULU	AKULA SRIRAMULU
COLLEGE OF ENGG	COLLEGE OF ENGG	COLLEGE OF ENGG
TANUKU, AP, INDIA	TANUKU, AP, INDIA	TANUKU, AP, INDIA

ABSTRACT

It has long been recognized that complete jamming of wireless networks can be realized by generating continuous noise with sufficient power in the vicinity of the wireless network. There are many disadvantages of this approach including high energy requirements and a high probability of detection. The purpose of this paper is to show that similar jamming effectiveness can be achieved with very low energy requirements and low probability of detection. We discuss various measures of performance for jamming and the role of authentication in denial of service attacks. Then we study and simulate, using OPNET 11.5, the effect of periodic jamming on throughput for an 802.11b network. We add *intelligence* to the jammer by using knowledge of the protocol and exploiting crucial timings and control packets. Intelligent jamming is shown to be more efficient than continuous jamming in terms of signal duration. We demonstrate the network's ability to estimate the impact of jamming and incorporate these estimates into the traffic allocation problem. Finally, we simulate the achievable throughput using our proposed traffic allocation method in several scenarios.

Keywords: DDOS ATTACKS, INTELLIGENT JAMMERS, 802.11B NETWORKS

INTRODUCTION

Wireless networks now enjoy widespread commercial implementation because of their low cost, ease of use and setup. Wireless access point based 802.11b hotspots are commonplace with more and more mobile users accessing the Internet wirelessly through various high-end mobile devices already available in the market at affordable prices. However, since accessing wireless media is much easier than tapping a wired network, security becomes a serious concern when implementing any wireless network. are among hundreds of articles that deal mainly with confidentiality and authentication related security attacks. We consider a particular class of Denial of Service (DoS) *jamming*. For our purposes, jamming is any attack to deny service to legitimate users by generating noise or fake protocol packets or legitimate packets but with spurious timing. The jamming results in focused primarily on energy conservation and in some cases were heavily dependent on the TCP performance. The results presented here do not depend on any layer above the MAC layer. This is an appropriate way to test MAC layer DoS attacks. The role of TCP in DoS attacks is the subject of another study. The most trivial way of disrupting a wireless network is by generating a continuous high power noise across the entire bandwidth near the transmitting and/or receiving nodes. The device that generates such a noise is called a *jammer* and the process is called *jamming*. However, jamming can be made more energy efficient and less detectable if the jammer operates using knowledge of the protocol. Energy efficient stealthy jammers are a goal. We will show how the jammer can briefly disrupt selected control packets and reduce network throughput to zero if need be. Such jammers, which jam the network with the knowledge of the protocol, are termed as protocol aware jammers. Jamming and its countermeasures have a long history in military applications.

2. Proposed Security Schemes Against Jamming in WSNs

The security schemes proposed in the WSN literature to address jamming issue can be categorized in

I. detection techniques,
II. proactive countermeasures,
III. reactive countermeasures, and

IV. Mobile agent (MA)-based countermeasures.

In the following lines, we will briefly present each category along with its corresponding approaches.

The relevant advantages and disadvantages of each approach are highlighted and evaluated.

2.1. Detection Techniques

The purpose of detection techniques is to instantly detect jamming attacks. The approaches of this category cannot cope with jamming alone; they can significantly enhance jamming protection only when used in conjunction with other countermeasures by providing valuable data (e.g., the initiation and type of jamming attack).

2.1.1. Radio interference detection in Wireless sensor network

Radio interference relations among the nodes of a wireless sensor network (WSN) and the design of a radio interference detection protocol (RID) are discussed in Reference [4]. However, jamming from external sources is not investigated; hence RID remains highly vulnerable from jamming attacks.

2.1.2. The feasibility of launching and Detecting jamming attacks in WSNs

In Reference [5] Xu *et al*. claim that understanding the nature of jamming attacks is critical to assuring the operation of wireless networks, so their focus is on the analysis and detection of jamming signals and they do not deal with effective countermeasures against jamming.

2.3. Reactive Countermeasures

The main characteristic of reactive countermeasures is that they enable reaction only upon the incident of a jamming attack sensed by the WSN nodes. Thus they need reduced computational and energy cost compared to proactive countermeasures but in the case of stealth or deceptive jamming there is a great possibility for delayed sensing of jamming.

2.3.1. JAM

Wood and Stankovic propose the detection and mapping of jammed regions [11] to increase network efficiency. However, this method presents several drawbacks: first, it cannot practically defend in the scenario that the attacker jams the entire WSN or a significant percentage of nodes; second, in the case that the attacker targets some specific nodes (e.g., those that guard a security entrance) to obstruct their data transmission, again this technique fails to protect nodes under attack.

2.3.2. Channel surfing and spatial retreat

Xu *et al*. in Reference [12] proposed two evasion strategies against constant jammers: channel surfing and spartial retreat. Channel surfing is essentially an adaptive form of FHSS. Instead of hopping continuously from one channel to another, a node switches to a different channel only when it discovers that the current channel is being jammed. Spartial retreat is an algorithm according to which two nodes move in Manhattan distances to escape from a jammed region. The main shortcoming of the two Abovementioned strategies is that they are effective only against constant jammers and they have no results against more intelligent or follow-on jammers.

2.3.3. Wormhole-based anti-jamming techniques in sensor networks

The basic idea is that jammed nodes use channel diversity in order to establish a communication with another node outside the jammed area. The authors propose three types of wormholes: (a) wired pair of sensors (b) frequency hopping pairs, and (c) uncoordinated channel-hopping.

In summary, wormholes may be an interesting idea to defend against jamming attacks but many problems still remain, as increased cost, the need for a large amount of time for the deployment of the sensor nodes in large scale WSNs and the fact that FHSS alone is not an effective countermeasure against fast-follower jammers [2]. 2.4. Mobile Agent-based Solutions This class of anti-jamming approaches enables MAs to enhance the survivability of WSNs. The term MA [14] refers to an autonomous program with the ability to move from host to host and act on behalf of users toward the completion of an assigned task. MA-based solutions do not require the use of specialized hardware. However, in conjunction with spread spectrum hardware their anti-jamming properties can be significantly improved.

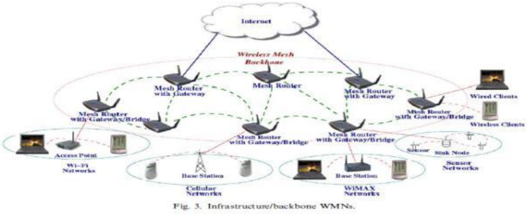


Fig 1: Anti jamming architecture

3. Network architecture

The basic architecture is shown in Fig. 4. In Client WMNs, a packet destined to a node in the network hops through multiple nodes to reach the destination. Client WMNs are

3.1 Hybrid WMNs

This architecture is the combination of infrastructure and client meshing as shown in Fig. 5. Mesh clients can access the network through mesh routers as well as The combination of free spectrum, efficient channel coding and cheap interface hardware has made 802.11-based access networks extremely popular.

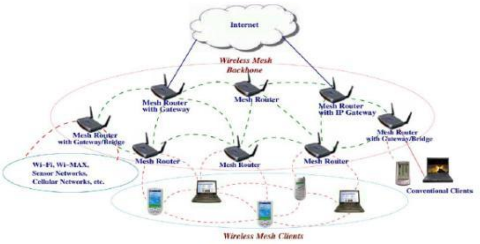

Internet
Wireless Mesh Backbone
Mesh Router with Gateway
Mesh Router
Mesh Router with IP Gateway
Mesh Router with Gateway/Bridge
Mesh Router with Gateway/Bridge
Mesh Router
Mesh Router
Mesh Router
Wi-Fi, Wi-MAX, Sensor Networks, Cellular Networks, etc.
Conventional Clients
Wireless Mesh Clients

Fig. 5. Hybrid WMNs.

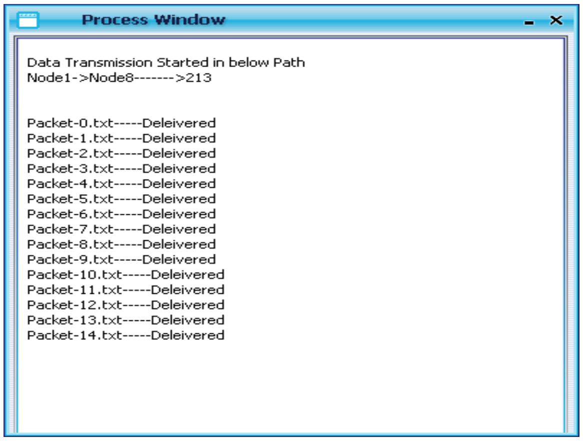
Fig 2: Hybrid Mesh networks

For a couple hundred dollars a user can buy an 802.11 access point that seamlessly extends their existing network connectivity for almost 100 meters. As a result, the market for 802.11-based LANs exceeded $1 directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, Wi MAX, cellular, and sensor networks; the routing capabilities of clients provide improved connectivity and coverage inside the WMN. The hybrid architecture will be the most applicable case in our opinion.

3.2 802.11 Denials-of-Service Attacks: Real Vulnerabilities and Practical Solutions

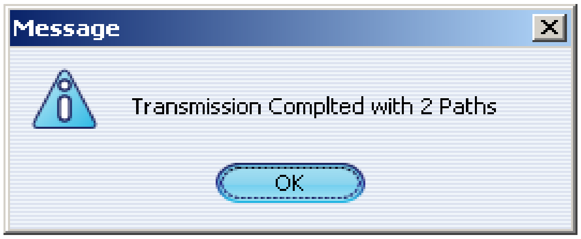
Billion in 2001 and includes widespread use in the home, enterprise and government/military sectors, as well as an emerging market in public area wireless networks. However, this same widespread deployment makes 802.11-based networks an attractive target for potential attackers. Indeed, recent research has demonstrated basic flaws in 802.11's encryption mechanisms and authentication protocols ultimately leading to the creation of a series of protocol extensions and replacements (e.g., WPA, 802.11i, 802.1X) to address these problems. However, most of this work has focused primarily on the requirements of access control and confidentiality, rather than availability. In contrast, this paper focuses on the threats posed by denial-of-service (DoS) attacks against 802.11's MAC protocol. Such attacks, which prevent legitimate users from accessing the network, are a vexing problem in all networks, but they are particularly threatening in the wireless context. Without a physical infrastructure, an attacker is afforded considerable flexibility in deciding where and when to attack, as well as enhanced anonymity due to the difficulty in locating the source of individual wireless transmissions. Moreover, the relative immaturity of 802.11-based network management tools makes it unlikely that a well-planned attack will be quickly diagnosed. Finally, as we will show, vulnerabilities in the 802.11 MAC protocol allow an attacker to selectively or completely disrupt service to the network using relatively few packets and low power consumption.

Results and Discussions:



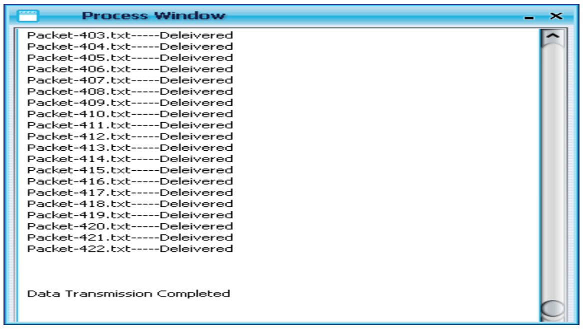
```
Data Transmission Started in below Path
Node1->Node8------->213


Packet-0.txt-----Deleivered
Packet-1.txt-----Deleivered
Packet-2.txt-----Deleivered
Packet-3.txt-----Deleivered
Packet-4.txt-----Deleivered
Packet-5.txt-----Deleivered
Packet-6.txt-----Deleivered
Packet-7.txt-----Deleivered
Packet-8.txt-----Deleivered
Packet-9.txt-----Deleivered
Packet-10.txt-----Deleivered
Packet-11.txt-----Deleivered
Packet-12.txt-----Deleivered
Packet-13.txt-----Deleivered
Packet-14.txt-----Deleivered
```

Fig 3: Starts the transmission



Transmission Complted with 2 Paths

Fig 4: parallel paths selection process



```
Packet-403.txt-----Deleivered
Packet-404.txt-----Deleivered
Packet-405.txt-----Deleivered
Packet-406.txt-----Deleivered
Packet-407.txt-----Deleivered
Packet-408.txt-----Deleivered
Packet-409.txt-----Deleivered
Packet-410.txt-----Deleivered
Packet-411.txt-----Deleivered
Packet-412.txt-----Deleivered
Packet-413.txt-----Deleivered
Packet-414.txt-----Deleivered
Packet-415.txt-----Deleivered
Packet-416.txt-----Deleivered
Packet-417.txt-----Deleivered
Packet-418.txt-----Deleivered
Packet-419.txt-----Deleivered
Packet-420.txt-----Deleivered
Packet-421.txt-----Deleivered
Packet-422.txt-----Deleivered


Data Transmission Completed
```

Fig 5: transmission completed

CONCLUSIONS:

We studied various protocols aware jamming attacks that can be launched in an access point based 802.11b network. We started by presenting the various jamming attacks ranging from trivial jamming to intelligent jamming attacks such as CTS corrupt jamming. We then presented simulation results showing the effect of misbehaving nodes that do not adhere to the underlying MAC protocol. The network throughput suffered drastically even in the presence of a single misbehaving node and more so with two misbehaving nodes. We then presented several hybrid attacks that increase the effectiveness of the attack or the decrease the probability of detection of the attack.

REFERENCES

[1] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless mesh networks: A survey,” *Comput. Netw.*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[2] E. M. Sozer, M. Stojanovic, and J. G. Proakis, “Underwater acoustic networks,” *IEEE J. Ocean. Eng.*, vol. 25, no. 1, pp. 72–83, Jan. 2000.

[3] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: Wiley, 2001.

[4] J. Bellardo and S. Savage, “802.11 denial-of-service attacks: Real vulnerabilities and practical solutions,” in *Proc. USENIX Security Symp.*, Washington, DC, Aug. 2003, pp. 15–28.

[5] D. J. Thuente and M. Acharya, “Intelligent jamming in wireless networks with applications to 802.11 b and other networks,” in *Proc. 25th IEEE MILCOM*, Washington, DC, Oct. 2006, pp. 1 7.

[6] A. D.Wood and J. A. Stankovic, “Denial of service in sensor networks,” *Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[7] G. Lin and G. Noubir, “On link layer denial of service in data wireless LANs,”*Wireless Commun. Mobile Comput.*, vol. 5, no. 3, pp. 273–284, May 2005.

[8] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks: Attack and defense strategies,” *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[9] D. B. Johnson, D. A. Maltz, and J. Broch, *DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks*. Reading, MA: Addison-Wesley, 2001, ch. 5, pp. 139–172.

[10] E. M. Royer and C. E. Perkins, “Ad hoc on-demand distance vector routing,” in *Proc. 2nd IEEE WMCSA*, New Orleans, LA, Feb. 1999, pp. 90–100.