International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 3, Issue 1 (August 2013) PP: 13-16

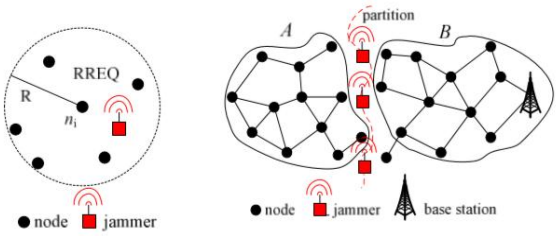
Container-Beating Approaches for Avoiding Discriminative Cramming Assaults

P. Obulamma[1], P. Venkata Ramanaiah[2], P. Sreenivasulu[3]
1, 3. M.Tech student, 2.Assistant Professor
Global College of Engineering & Technology, Kadapa

Abstract: *Modern society is heavily dependent on wireless networks for providing voice and data communications. Wireless data broadcast has recently emerged as an attractive way to disseminate data to a large number of clients. Typically, jamming has been addressed under an external threat model. In this work, we address theproblem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. Jammingis broken down into layers and this paper focuses on jamming at the Transport/Network layer.Our method differs from classicfrequency hopping in that no two nodes share the same hop- ping sequence, thus mitigating the impact of node compromise. To mitigate jamming attacks, we develop three schemes that preventreal-time packet classification by combining cryptographic primitives with physical-layer attributes.*

I. Introduction

In this paper, we investigate an attack where the attacker masks the event (event masking) that the sensor network should detect by stealthily jamming an appropriate subset of the nodes.While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter.From a security point of view, convergence on a preas- signed control channel constitutes a single point of failure. An adversary can severely degrade the network performance by launching a Denial of Service (DoS) attack on the control channel, thus negating any gain due to the availability of multiple data channels.The impact of control-channel jamming in ad hoc net- works can propagate way beyond the physical jamming range of an adversary, defined as the area within which packets are corrupted due to jamming.



We propose another solution which instead of mapping the control channels to static locations (in terms of timeslot, frequency), it randomly maps them according to a crypto- graphic function.As a result, the external attacker will have to jam blindly which is either energy inefficient or less effective.Jamming can be viewed as a form of Denial-of-Service (DoS) attack, whose goal is to prevent users from receiving timely and adequate information.

Wireless Data Broadcast Systems:

Wireless data broadcast has recently emerged as an attractive way to disseminate data to a large number of clients.This approach enables the system to serve a large number of heterogeneous clients, minimizing client power consumption as well as protecting the privacy of the clients' locations.

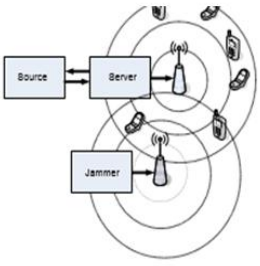


Fig. 1. A typical data broadcast system.

Trouble report and hypothesis:

The fallowing are different models in this to specify problem statement of how to hide the packets.

Network model:

The network consists of a collection of nodes connected via wireless links.Nodes communicate both in unicast mode and broadcast mode.

Communication Model:

Packets are transmitted at a rate of R bauds. Each PHY-layer symbol corresponds to q bits, where the value of q is defined by the underlying digital modulation scheme.

Enthusiasm:

In a wireless sensor network, all mutual communication between sensors and between the network operator and sensors is wireless.Furthermore, even if jamming is detected, the network operator still cannot precisely locate the adversary; only the boundary of the jamming region can be determined.

Our goal is to build a wireless link layer protocol that al- lows clients and services to communicate without exposing identifiers to third parties.The impact of control-channel jamming in ad hoc net- works can propagate way beyond the physical jamming range of an adversary, defined as the area within which packets are corrupted due to jamming. For example, the adversary may choose to jam the request-to-send (RTS) and clear-to-send (CTS) messages at the MAC layer so that the medium access delay is significantly increased.This internal adversary model is realistic for network architectures such as mobile ad-hoc, mesh, cognitive radio, and wireless sensor networks, where network devices may operate unattended.

II. LITERATURE SURVEY

In today's world large volume of data is being stored and transmitted electronically; it is no surprise that various methods of protecting or hiding such data have evolved.One lesser-known but rapidly growing method is steganography, the art and science of hidinginformation so that it does not even appear to exist.In addition, various other techniques have been proposed for hiding the data at rest for example hiding data in the slack space and digital warrens. Although, these techniques differ from each other but their main purposed is to provide privacy, integrity and security by hiding the data in some way.

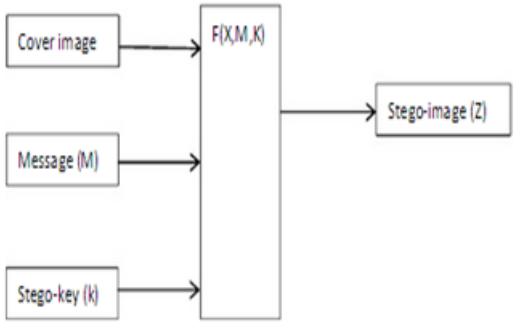
The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. Slack space is another technique that is used to hide information in the unallocated space of the disks. This unallocated space is some time called as logical end of the file or end of the associated cluster. Hiding the file or data in the slack space has some advantages like, the host or the carrier file is unaffected while the hidden data is transparent to the host OS and file manager.

The important concept from this history lesson is that communication does not have to occur over standard open channels using well-known methods. The Internet, in its massive, protocol-laden glory, is a playground for the modern steganographer. For example, think of an IP packet as the wax tablet previously mentioned.

Techniques for hiding data while communicating:

Steganography:

Steganography is the art and science of hiding communication; steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography.



III. Cryptography

Today, secure communication is necessary on the internet or web and for making the communication secure there is a need of some technique which can maintain the privacy and security in the communication. Keeping all this in mind a technique called cryptography has been proposed. With the help of cryptography a sender can encrypt a massage with a small piece of information and then send the encrypted message to the receiver. The receiver decrypts the encrypted message by the key that has been shared and recover the original message.

Categories of cryptographic system:

1. Symmetric key ciphers: in this approach sender and receiver use the same secret key for encryption and decryption of messages.
2. Public key ciphers: are also known as asymmetric algorithms, in this approach the key used for encryption is different from the key used for decryption

IV. RELATED WORK

Wireless networks are highly sensitive to denial of service attacks.The traditional anti-jamming strategy has been extensively relying on spread spectrum technique.We use results from coding theory to assign keys in our approach that guarantees the resilience and identification of traitors. The problem of control channel jamming in the presence of node compromise was previously addressed in the con- text of GSM networks. They proposed frequency hopping to avoid jamming, but assumed that all cryptographic quantities are se- cure. However, in our scheme, hopping sequences are designed to implement the control channel, while in UFH hopping sequence are purely random.

In this work, they propose a proactive protocol that first detects and then maps the jammed area. In their approach, each node is assumed to have a detection-module that periodically returns a jammed or unjammed message. They show that reliable detection can be a challenging task in wireless sensor networks.In the context of digital communications, the jamming problem has been addressed under various threat models.

Preceding job Selective blocking:

To perform packet classification, the adversary exploits inter-packet timing information to infer eminent packet transmissions. Selective jamming attacks have been experimentally implemented using software-defined radio engines.

Non-Selective Jamming Attacks:

Conventional methods for mitigating jamming employ some form of SS communications. They also pro- posed, a jamming-resistant broadcast method in whichtransmissions are spread according to PN codes randomly selected from a public codebook. Its protocol also uses sym- metric key cryptography to compute temporary addresses. However, it is not a general mechanism for packet delivery and is not authenticated like Tryst.

Different types of jamming attacks against wireless networks:

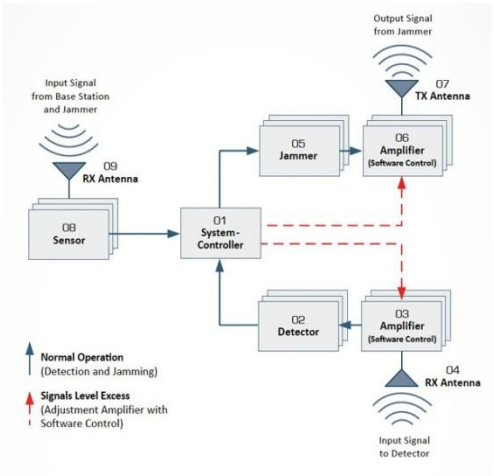
Based on the shared characteristics of the wireless medium, a wireless network can be easily affected by jamming attacks, which is one of the most effective forms of denial-of service (DoS) attacks against this type of networking architecture. Attacks can be implemented by either corrupting the operations of the medium access control (MAC) protocols or transmitting large amounts of interfering wireless signals without obeying the MAC protocols.

Physical Jamming:

Physical or Radio jamming in a wireless medium is a simple but disruptive form of DoS attack. These attacks are launched by either continuous emission of radio signals or by sending random bits onto the channel.

Virtual Jamming:

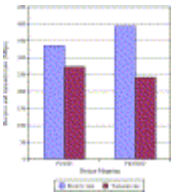
In IEEE 802.11 based MAC protocols, virtual carrier sensing is used at the MAC layer to determine the availability of the wireless medium. Jamming can be launched at the MAC layer through attacks on the RTS/CTS frames or DATA frames.

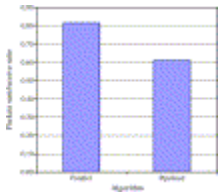


Mobile ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security- sensitive operations are still the main applications of ad hoc networks.

Performance analysis of Packet-Hiding techniques:

Multi-field packet classification is frequently performed by network devices such as edge routers and firewalls—such devices can utilize programmable network processors to perform this compute-intensive task at nearly line speeds. Nowadays packet classification is a fundamental task for network devices such as edge routers, firewalls and intrusion detection systems. Therefore packet classification is becoming more and more complex, with more flexibility and higher performance requirements.





In this work, we address theproblem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing.

V. CONCLUSION

We addressed the problem of control-channel jamming inmulti-channel ad hoc networks, under node compromise. We proposed a randomized distributed channel establishment scheme that allows nodes to select a new control channel using frequency hopping. We focus on combating powerful jammers that have full knowledge about the data distribution system. For suchjammers, the standard anti-jamming methods, such as spread-spectrum transmissions are not sufficient in order to guarantee timely delivery of the data, hence additional encoding is required at the packet level. We showed that the jammer canclassify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. We evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. We analyzed the security of our schemes and quantified their computational and communication overhead.

REFERENCES

[1] T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.

[2] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based anti jamming Techniques in sensor networks. IEEE Transactions on MobileComputing, 6(1):100–114, 2007.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors.

[4] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer Jamming attacks against WSN MAC protocols. ACMTransactions on Sensors Networks, 5(1):1–38, 2009.

[5] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network.