Detection of Jamming Attacks in Time Critical Wireless Applications Using Gambling Based Modeling

[1]Dr. Stephen Thangaraj, Dhanalakshmi Srinivasan College of Engineering and Technology

[2]Mr. S. Niresh Kumar, Dhanalakshmi Srinivasan College of Engineering and Technology

[3]Mrs. M. Revathi, Asan Memorial College of Engineering and Technology

Abstract

Wireless networking has been emerging for cyber-physical systems, especially the smart grid, has been drawing increasing attention therein it's broad applications for time-critical message delivery among electronic devices on physical infrastructures. We are going to develop the Detection Of Jamming Attacks In Time Critical Wireless Applications Using Gambling Based Modeling. The wireless channels exposes the messages in transit to jamming attacks, which broadcast radio interference to affect the network availability of electronic equipment's. Our paper focuses on similarity between the behavior of a jammer who attempts to disrupt the delivery of a time-critical message and thus the behavior of a gambler who intends to win a game of chance . Therefore, by gambling-based modeling and real-time experiments, we are going to identify the existance of phase transition phenomenon for successful time-critical message delivery under a selection of jamming attacks. Our objective during

1. INTRODUCTION

1.1. MOBILE COMPUTING

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal

1.2. MOBILE COMPUTING DESCRIPTION

Mobile Computing is "taking a computer and all necessary files and software out into the field". There are several different dimensions under which mobile computers can be defined: 1. In terms of physical dimensions; 2. In terms of how devices may be hosted; 3. In terms of when the mobility occurs; 4. In terms of Area Network, Wireless Personal Area Network or a piconet. Depending on the type of application the mobile computer runs, the computation of the applications may run only locally, e.g., a PC game. The majority of mobile computers for personal use tends to be used for communication or for remote data downloads such as remote Web access (see Mobile Internet device). As some mobile computers contain an array of sensors, microphones and cameras, these can be used for local data capture, filtering tagging and remote uploads. Increasing mobile computers are also being used to access services such as travel, payment or for access to controlled physical spaces.

1.3. MOBILE COMPUTING DEVICES

Some of the most common forms of mobile computing devices are as follows.Portable computers, compacted lightweight units including a full character set keyboard and primarily intended as hosts for software that may be parametrized, as laptops, notebooks, notepads, etc.Mobile phones including a restricted key primarily intended but not restricted to for vocal communications, as cell phones, smart phones, phonepads, etc.Smart cards that can run multiple applications but typically payment, travel and scure area accessWearable computers, mostly limited to functional keys and primarily intended as incorporation of software agents, as watches, wristbands, necklaces, keyless implants, etc.The existence of these classes is expected to be long lasting, and complementary in personal usage, none replacing one the other in all features of convenience.

2. SYSTEM ANALYSIS

2.1. EXISTING SYSTEM

There are two key observations that drive our modeling of reactive and non-reactive jammers. (i) In a time critical application, a message becomes invalid as long as the message delay D is greater than its delay threshold σ. Thus, to define a metric, message invalidation ratio, to quantify the impact of jamming attacks against the time critical application. (ii) When a retransmission mechanism is adopted, to successfully disrupt the delivery of a time-critical message, the jammer needs to jam each transmission attempt of this message until the delay D is greater than σ. As a result, such behavior of the jammer is exactly the same as the behavior of a gambler who intends to win each play in a game to collect enough fortune to achieve his gambling goal of σ dollars.

2.1.1. DRAWBACKS OF EXISTING SYSTEM

Broadcast communications are particularly vulnerable under an internal¬ threat model because all intended receivers must be aware of the secrets used to protect transmissions. The open nature of the wireless medium leaves it vulnerable to intentional¬ interference attacks, typically referred to as jamming. Anyone with a transceiver can eavesdrop on wireless transmissions, inject¬ spurious messages, or jam legitimate ones. Hence, the compromise of a single receiver is sufficient to reveal relevant¬ cryptographic information.

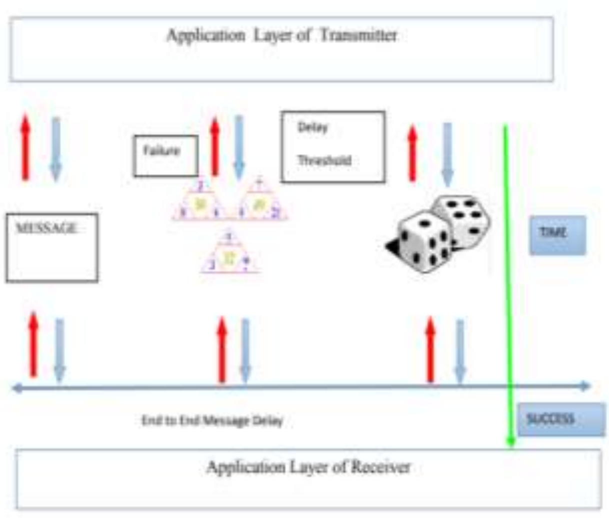
2.2. PROPOSED SYSTEM

To develop a gambling-based model to derive the message invalidation ratio of the time-critical application under jamming attacks. To validate our analysis and further evaluate the impact of jamming attacks on an experimental power substation network by examining a set of use cases specified by the National Institute of Standards and Technology (NIST). Based on theoretical and experimental results, To design the jamming attack detection based on estimation (JADE) system to achieve efficient and reliable jamming detection for the experimental substation network. Our contributions in this paper are threefold. For reactive jamming, find that there exists a phase transition phenomenon of message delivery performance: when jamming probability p (the probability that a physical transmission is jammed) increases, the message invalidation ratio first increases slightly (and is negligible in practice), then increases dramatically to 1. For non-reactive jamming, there exists a similar phenomenon: when the average jamming interval (the time interval between two non-reactive jamming pulses) increases, the message invalidation ratio first has the value of 1, then decreases dramatically to 0.

2.2.1. ADVANTAGES

Relatively easy to actualize by exploiting knowledge of network protocols¬ and cryptographic primitives extracted from compromised nodes. Our findings indicate that selective jamming attacks lead to a DoS with very low effort on behalf of the jammer. Achieve strong security properties.

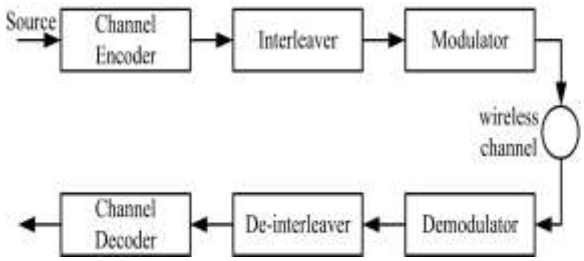
3. SYSTEM DESIGN



preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in un-cast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using pre-shared pair-wise keys or asymmetric cryptography.

Real time packet classification

Consider the generic communication system depicted in Fig. At the PHYlayer, a packet m is encoded, interleaved, and modulated before it is transmittedover the wireless channel. At the receiver, the signal is demodulated, deinterleaved,and decoded, to recover the original packet m.



attacker targeted a TCP connectionestablished over a multi-hop wireless route. In the second scenario, the jammertargeted network-layer control messages transmitted during the route establishmentprocess selective jamming would be the encryption of transmitted packets(including headers) with a static key. However, for broadcast communications, thisstatic decryption key must be known to all intended receivers and hence, issusceptible to compromise. An adversary in possession of the decryption key canstart decrypting as early as the reception of the first cipher text block.

STRONG HIDING COMMITMENT SCHEME (SHCS)

In this paropose a strong hiding commitment scheme (SHCS), whichis based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to aminimum.The computation overhead of SHCS is one symmetric encryption at the
sender and one symmetric decryption at the receiver. Because the headerinformation is permuted as a trailer and encrypted, all receivers in the vicinity of asender must receive the entire packet and decrypt it, before the packet type anddestination can be determined. However, in wireless protocols such as 802.11, thecomplete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed. If some parts of the MAC header are
deemed not to be useful information to the jammer, they can remain unencrypted in
the header of the packet, thus avoiding the decryption operation at the receiver.

CRYPTOGRAPHIC PUZZLE HIDING SCHEME (CPHS)

Present a packet hiding scheme based on cryptographic puzzles. Themain idea behind such puzzles is to force the recipient of a puzzle execute a predefinedset of computations before he is able to extract a secret of interest. Thetime required for obtaining the solution of a puzzle depends on its hardness and thecomputational ability of the solver. The advantage of the puzzle based scheme isthat its security does not rely on the PHY layer parameters. However, it has highercomputation and communication overhead. consider several puzzle schemes as thebasis for CPHS. For each scheme, analyze the implementation details whichimpact security and performance. Cryptographic puzzles are primitives originallysuggested by Merkle as a method for establishing a secret over an insecurechannel.

4. CONCLUSION

An internal adversary model in which the jammer is part of the networkunder attack, thus being aware of the protocol specifications and shared networksecrets. Then showed that the jammer can classify transmitted packets in real timeby decoding the first few symbols of an ongoing transmission. evaluating theimpact of selective jamming attacks on network protocols such as TCP androuting. Our findings show that a selective jammer can significantly impactperformance with very low effort. To developed three schemes that transform aselective jammer to a random one by preventing real-time packet classification.

FUTURE ENHANCEMENT

Here prevent jamming attacks in particular network. In future work willprevent jamming attacks in more networks and add broadcasting facility tomultiple client and server.

5. REFERECES

[1] Y.W. Law, M. Palaniswami, L.V. Hoesel, J. Doumen, P. Hartel, and P.Havinga, (2009)"Energy-Efficient Link-Layer Jamming Attacks against WSN

MAC Protocols," ACM Trans. Sensor Networks, vol. 5, no. 1, pp. 1-38.

[2] L. Lazos, S. Liu, and M. Krunz,(2009) "Mitigating Control-Channel Jamming Attacks in Multi- Channel Ad Hoc Networks," Proc. Second ACM Conf. Wireless Network Security, pp. 169-180.

[3] Y. Liu, P. Ning, H. Dai, and A. Liu(2010), "Randomized Differential DSSS:
Jamming- Resistant Wireless Broadcast Communication," Proc. IEEE INFOCOM,
2010.

[4] B. Schneier,(2007) Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.

[5] B. Thapa, G. Noubir, R. Rajaramanand, and B. Sheng,(2011) "On theRobustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming,".