International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 3 1290 – 1293

Jamming Attack Detection and Evaluating Using Wireless Application

Sivagami.S[1],Poornima Mohapatra.B[2],Priya darshini.G.R[3],Charukeerthy.V.S
[1]Assistant professor, [2,3,4] Students, Department of Information Technology
[1,2,3,4] Velammal Institute of Technology, Chennai - 601 204

Abstract:- When data is transferred from one host to another host,attacker may try to attack the packet or data which is in transit.Inorder to avoid such kind of attack in time critical wireless application and delivery message securely in wireless application. In this paper, we aim at modeling and detecting jamming attacks against time-critical wireless networks.To measure network performance ,packet loss and throughput metrics are used . To quantify the performance of time-critical applications,message invalidation ratio metric are used. This approach is inspired by the similarity between the behavior of a jammer who attempts to disrupt the delivery of a message and the behavior of a gambler who intends to win a gambling game. By gambling-based modeling and real-time modules, we can successful delivery time-critical message under a variety of jamming attacks.

Keywords: *Access control, Data security, privacy.*

*****

I. INTRODUCTION

Today's wireless technologies have brought benefit to people's life, such as mobile messaging,wifi and gaming. On the other side, it also enables a new emerging cyber-physical systems, in particular for the smart grid where the attacker may try to disprupt message in wireless application.Throughput metrics that measures how much data can be delivered within a time period, wireless networking for cyber-physical systems aims at offering reliable and timely message delivery between physical devices. In such systems, a large amount of data sent in wireless network which may lead to traffic is time-critical Due to traffic it may lead to failures of system operations, and other failures. For instance, in the smart grid, a binary result of fault detection on a power feeder can trigger subsequent operations of circuit breakers. If the message does not arrive on time or it is missed, the action may be delayed, which can cause fault propagation along physical infrastructures and potential damages to power equipments.Therefore it is importance to guarantee network to avail message delay performance instead of data throughput performance in such time-critical applications.In the shared nature of wireless channels inevitably surrenders message to jamming attacks, which may affect the performance and reliability[2]-[5].

Although there have been significant advances towards jamming characterization and counter measures for conventional networks, little attention has been focused on jamming against message delivery in time-critical wireless applications. In particular, conventional performance metrics cannot be readily adapted to measure the jamming impact against time critical messages. In wireless network ,the jamming attacks is evaluated at the packet level.

II. LITERATURE SURVEY

1) Literature Review: On Network Performance Evaluation toward the Smart Grid: A Case Study of DNP3 over TCP/IP

The smart grid is the next-generation power system that incorporates power infrastructures with information technologies[1]. In the smart grid, power devices are interconnected to support a variety of intelligent mechanisms, such as relay protection and demand response. To enable such mechanisms, messages must be delivered in a timely manner via network protocols. A cost-efficient and backward-compatible way for smart grid protocol design is to migrate current protocols in supervisory control and data acquisition (SCADA) systems to the smart grid. However, an open question is whether the performance of SCADA protocols can meet the timing requirements of smart grid applications. To address this issue, we establish a micro smart grid, Green Hub, to measure the delay performance of a predominant SCADA protocol, distributed network protocol 3.0 (DNP3) over TCP/IP. Our results show that although DNP3 over TCP/IP is widely considered as a smart grid communication protocol, it cannot be used in applications with delay constraints smaller than 16ms in Green Hub, such as relay protection. In addition, since DNP3 provides reliability mechanisms similar to TCP, we identify that such an overlapped design induces 50%-80% of the processing delay in embedded power devices. Our results indicate that DNP3 over TCP/IP can be further optimized in terms of delay efficiency, and a lightweight communication protocol is essential for time-critical smart grid applications.

2)Literature Review: The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks

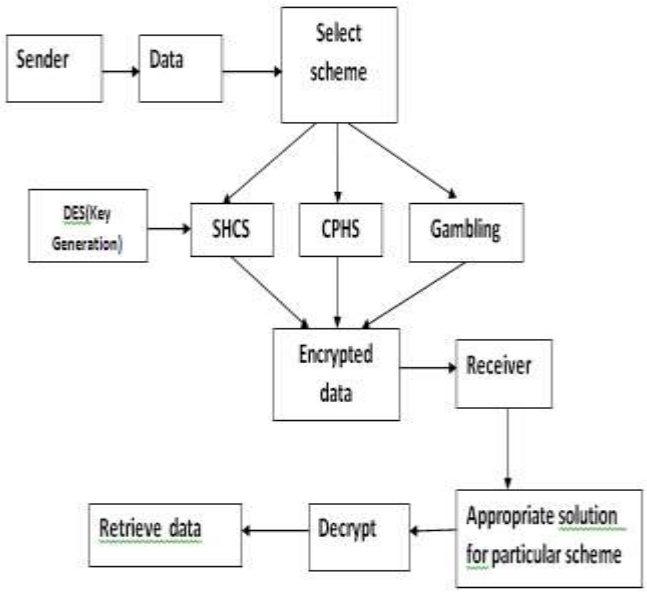
Wireless networks are built upon a shared medium that makes it easy for adversaries to launch jamming-style

attacks. These attacks can be easily accomplished by an adversary emitting radio frequency signals that do not follow an underlying MAC protocol. Jamming attacks can severely interfere with the normal operation of wireless networks and, consequently, mechanisms are needed that can cope with jamming attacks. In this paper, we examine radio interference attacks from both sides of the issue: first, we study the problem of conducting radio interference attacks on wireless networks, and second we examine the critical issue of diagnosing the presence of jamming attacks. Specifically, we propose four different jamming attack models that can be used by an adversary to disable the operation of a wireless network, and evaluate their effectiveness in terms of how each method affects the ability of a wireless node to send and receive packets. We then discuss different measurements that serve as the basis for detecting a jamming attack, and explore scenarios where each measurement by itself is not enough to reliably classify the presence of a jamming attack. In particular, we observe that signal strength and carrier sensing time are unable to conclusively detect the presence of a jammer. Further, we observe that although by using packet delivery ratio we may differentiate between congested and jammed scenarios, we are nonetheless unable to conclude whether poor link utility is due to jamming or the mobility of nodes. The fact that no single measurement is sufficient for reliably classifying the presence of a jammer is an important observation, and necessitates the development of enhanced detection schemes that can remove ambiguity when detecting a jammer.

3) Literature Review: On the Performance of IEEE 802.11 under Jamming

In this paper, we study the performance of the IEEE 802.11 MAC protocol under a range of jammers that covers both channel-oblivious and channel-aware jamming. We study two channel-oblivious jammers: a periodic jammer that jams deterministically at a specified rate, and a memory less jammer whose signals arrive according to a Poisson process. We also develop new models for channel-aware jamming, including a reactive jammer that only jams non-colliding transmissions and an omniscient jammer that optimally adjusts its strategy according to current states of the participating nodes. Our study comprises of a theoretical analysis of the saturation throughput of 802.11 under jamming, an extensive simulation study, and a test bed to conduct real world experimentation of jamming IEEE 802.11 using GNU Radio and USRP platform. In our theoretical analysis, we use a discrete-time Markov chain analysis to derive formulae for the saturation throughput of IEEE 802.11 under memory less, reactive and omniscient jamming. One of our key results is a characterization of optimal omniscient jamming that establishes a lower bound on the saturation throughput of 802.11 under arbitrary jammer attacks. We validate the theoretical analysis by means of Qualnet simulations. Finally, we measure the real-world performance of periodic and memory less jammers using our GNU radio jammer prototype.

III. SYSTEM ARCHITECTURE



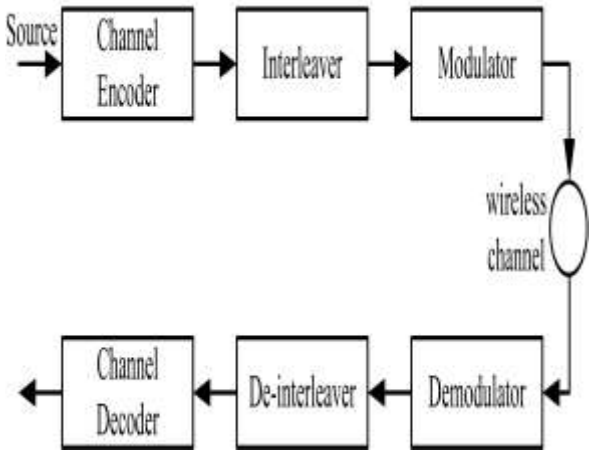
IV. MODULE DESCRIPTION

1. Real Time Packet Classification
2. Selective Jamming Module
3. Strong Hiding Commitment Scheme (SHCS)
4. Cryptographic Puzzle Hiding Scheme (CPHS)
5. Gambling-based model

The major functional components are briefly described below:

1. REAL TIME PACKET CLASSIFICATION:

As shown in the block diagram,the data or message is sent to channel encoder which encodes the data. After that it is interleaved which make system more efficient,fast and reliable by arranging data in non continguous manner and then it is modulated and passed through wireless channel.



At the receiver end,the data is demodulated and deinterleaved and then passed to channel deoder which decodes the data and produce original data.The above process are carried out in he physical PHY layer.The objective of the encryption key of a hiding scheme were to remain secret and maintain privacy, the static portions of a transmitted packet could potentially lead to packet classification. This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix.

2. SELECTIVE JAMMING MODULE:

Selective jamming is in which the attacker will targeted a particular node inorder to attack it and tries to get information from that particular node.We illustrate the impact of selective jamming attacks on the network performance.We have implemented selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process selective jamming would be the encryption of transmitted data with a static key. But for the broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. An adversary in possession of the decryption key can start decrypting as early as the reception of the first cipher text block.

3. STRONG HIDING COMMITMENT SCHEME (SHCS):

We propose a strong hiding commitment scheme (SHCS), which provides strong hiding property while keeping the computation and communication overhead to a minimum.This scheme is based on symmetry cryptography.

SHCS scheme which provide secure transmission of data by avoiding attack of data while in transmit.SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined. However, in wireless protocols such as 802.11, the complete 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.

4. CRYPTOGRAPHIC PUZZLE HIDING SCHEME (CPHS):

We present another scheme which provides packet hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle to solve puzzles or computations inorder to extract a secret of data. But the puzzles should be solved in given time interval.The time required for obtaining the solution of a puzzle depends on the computational ability of the solver. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters.If time limit exceeds,solver cannot retrieve data. However, it has higher computation and communication overhead. We consider several puzzle schemes as the basis for CPHS. For each scheme, we analyze the implementation details which impact security and performance. Cryptographic puzzles are primitives originally suggested by Merkle as a method for establishing a secret over an insecure channel.CPHS that provide secure transmission of data and to retrieve data the receiver need to solve the defined puzzles within time limit.

5. GAMBLING-BASED MODEL

We presented gambling based model .In this scheme it identifies the modification that are made to the packet or data.There are two observations, we develop a gambling-based model to derive the message invalidation ratio of the time-critical application under jamming attacks. This module is based on such as the behavior of a gambler who intends to win a gambling game and tries to retrieve data.We 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, we design the jamming attack detection based on estimation (JADE) system to achieve efficient and reliable jamming detection for the experimental substation network.

V. IMPLEMENTATION

Sun Microsystems officially licenses the Java Standard Edition platform for Linux, Mac OS X and Solaris. Although in the past Sun has licensed Java to Microsoft, the license has expired and has not been renewed. Through a network of third-party vendors and licensees, alternative Java environments are available for these and other platforms.

Sun's trademark license for usage of the Java brand insists that all implementations be "compatible". This resulted in a legal dispute with Microsoft after Sun claimed that the Microsoft implementation did not support RMI or JNI and had added platform-specific features of their own. Sun sued in 1997 and in 2001 won a settlement of $20 million as well as a court order enforcing the terms of the license from Sun. As a result, Microsoft no longer ships Java with Windows, and in recent versions of Windows, Internet Explorer cannot support Java applets without a third-party plug-in. Sun, and others, has made available free Java run-time systems for those and other versions of Windows.

Platform-independent Java is essential to the Java EE strategy, and an even more rigorous validation is required to certify an implementation. This environment enables portable server-side applications, such as Web services, Java Servlets, and Enterprise JavaBeans, as well as with embedded systems based on OSGi, using Embedded Java environments. Through the new GlassFish project, Sun is working to create a fully functional, unified open source implementation of the Java EE technologies.

Sun also distributes a superset of the JRE called the Java Development Kit (commonly known as the JDK), which includes development tools such as the Java compiler, Javadoc, Jar and debugger.

VI. CONCLUSION AND FUTURE WORK

Therefore in this paper ,we aim to delivery data or message securely in wireless application by avoiding the attacker which attack the data while in transmit.In Broadcast communications ,it is vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions i.e attack takesplace. 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.

REFERENCES

[1] Office of the National Coordinator for Smart Grid Interoperability, “NIST framework and roadmap for smart grid interoperability standards, release 1.0,” NIST Special Publication 1108, 2009.

[2] P. M. Kanabar, M. G. Kanabar, W. El-Khattam, T. S. Sidhu, and A. Shami, “Evaluation of communication technologies for IEC 61850 based distribution automation system with distributed energy resources,” in Proc. of IEEE PES General Meeting (PES ’09), July 2009

[3] B. Akyol, H. Kirkham, S. Clements, and M. Hadley, “A survey of wireless communications for the electric power system,” in Tech. Report, Pacific Northwest National Laboratory, Jan. 2010 .

[4] Wi-Fi Alliance, “WiFi for the smart grid: Mature, interoperable, security-protected technology for advanced utility management communications,” Sept. 2009

[5] NIST Smart Grid Homepage, “Smart grid panel agrees on standards and guidelines for wireless communication, meter upgrades,” News Release, Apr. 19 2011