ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Combining Cryptographic Primitives to Avert Overcrowding Attacks in Wireless Networks

S.Rajasekaran [1], M.Geetha[2]

Research Scholar, Dept. of CS, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[1]

Associate Professor, Department of BCA, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[2]

ABSTRACT: The Open Nature of wireless medium leaves an intentional interference attack, typically referred to as jamming. This intentional interference with wireless transmission launch pad for mounting Denial-Of-Service attack on wireless networks. Typically, jamming has been addresses under an external threat model. However, adversaries with internal knowledge of protocol specification and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this work we address the problem of jamming attacks and adversary is active for short period of time, selectively targeting the messages of high importance. We show that the selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. They are Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), All-Or-Nothing Transformation Hiding Schemes (AONTS-HS). Random key distribution methods are done along with three schemes to give more secured packet transmission in wireless networks.

KEYWORDS: Selective jamming, denial-of-service, wireless networks, packet classification.

I. INTRODUCTION

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eaves- dropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. Typically, jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high-power interference signals. However, adopting an "al- ways-on" strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect. Conventional ant-jamming techniques extensively on spread-spectrum communications, or some form of jamming evasion (e.g., slow frequency hopping or spatial retreats). SS techniques provide bit-level protection by spreading bits according to a secret pseudo noise (PN) code, Known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model. Potential disclosure of secrets due to node compromise neutralizes the gains of SS. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information. In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

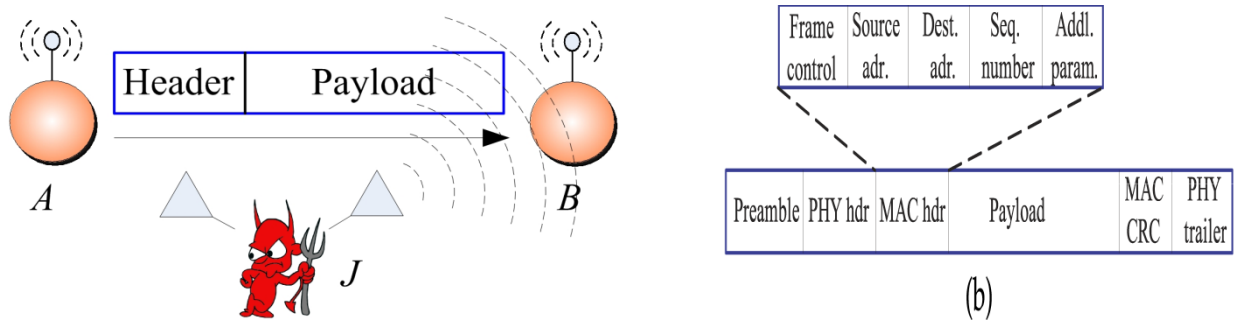
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

II. LITERATURE SURVEY

A Wireless networks are highly sensitive to denial of service attacks. The broadcast nature of wireless communication exposes the physical layer of the system to jamming. The traditional anti-jamming strategy has been extensively relying on spread spectrum technique. Very little work has been done from a system level to countermeasure jamming. In our previous work, we propose novel system architecture based on mechanism-hopping to increase the wireless network robustness against cross-layer jamming. Xu et al. study the effect and detection of jamming at MAC and PHY layer in wireless sensor networks. Resilience and identification of internal attackers is very difficult. To the best of our knowledge, we are the first to investigate the problem of control channel jamming by traitors. We use results from coding theory to assign keys in our approach that guarantees the resilience and identification of traitors. The rest of the paper is organized as follows.

In Section II, we present a scheme for a network with one traitor. In Section, we present a solution when there are up to traitors in the network. Section IV concludes the paper. We begin the paper in Section by providing an overview of our timing channel overlay. In Section, we show that detecting failed packet receptions is feasible, and thus our timing channel can be constructed. We next examine a simple single sender scenario in Section. Then we extend our timing channel to a multiple sender scenario, in Section. Finally, using our multi-sender timing channel, we explore the construction of an overlay link-layer in Section and discuss mechanisms that enhance the reliability of our over- lay. We wrap up the paper by discussing related work in Section, and provide concluding remarks.



(a)

Fig1. (a) Realization of a selective jamming attack. **(b)** A generic frame format for a wireless network.

III. EXISTING SYSTEM

RF interference has traditionally been addressed at the physical layer through modulation approaches (such as spread spectrum) with sufficiently powerful anti-jam margins to make disruption difficult. Unfortunately, such physical layer approaches are typically representative of military wireless systems and, for reasons of cost, are generally not employed in commodity wireless platforms

Disadvantages of existing system:

Under this model, jamming strategies include the continuous or random transmission of high power interference signals. However, adopting an "always-on" strategy has several disadvantages.

- First, the adversary has to expend a significant amount of energy to jam frequency bands of interest.
- Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

IV. PROPOSED SYSTEM

In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to end flow.target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to end flow.

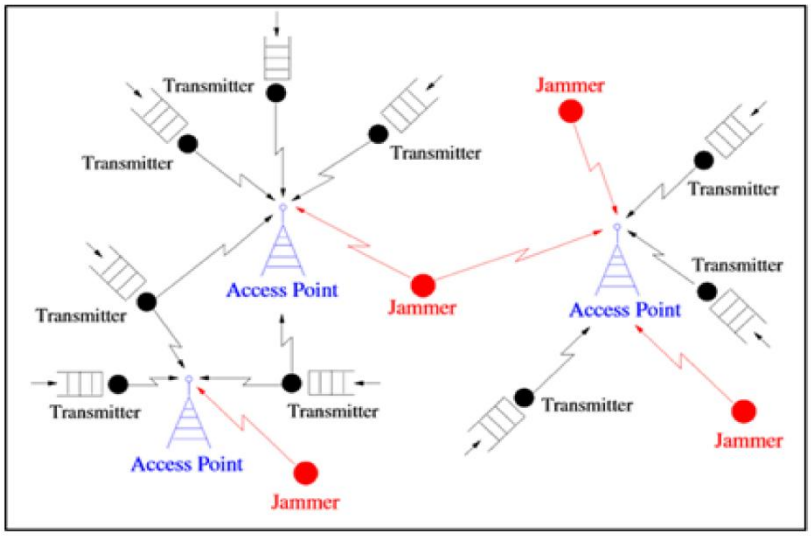


Fig 1.System Architecture

ADVANTAGES OF PROPOSED SYSTEM:

A random key distribution has been implemented to more secure the packet transmission in the wireless networks.

V. SYSTEM MODELS

NETWORK MODEL:

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 unicast mode and broadcast mode. Communications can be either unencrypted or encrypted. Symmetric keys are shared among all intended receivers in broadcast communication. These keys are established using preshared pair wise keys or asymmetric cryptography.

COMMUNICATION MODEL:

We present a packet-hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a predefined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and 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. However, it has higher computation and communication overheads. Let a sender S have a packet m for transmission. The senders select a random key k of desired length. S generates a puzzle P= puzzle(k,tp), where puzzle() denotes the puzzle generator function, and tp denotes the time required for the solution of the puzzle.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

RANDOM KEY DISTRIBUTION:
We propose the use of random key distribution to hide the location of control channels in time and/or frequency. We evaluate performance metrics of resilience to control channel jamming, identification of compromised users, and delay due to jamming as a function of the number of compromised users.

VI. ALGORITHM

BINARY ENCODING BASED KEY ASSIGNMENT (BBK)
In this section, we consider a system where there is only one traitor among N users. We present a 1-resilient scheme that requires 2 log N replications of control information. This scheme also allows us to uniquely identify the jammer. where f is a publically known cryptographic hashing function. User j knows the location of control signal at time slot f(k(i mod[log N]),i) by computing . The server computes a f table that stores the mapping of keys to channels at each timeslot. A legitimate user will succeed in accessing the control channel in a timeslot if no traitor jams that channel.

VII. COMPUTATION

Algorithm 1: BBK
Setup: N users, 1 traitor.
Result: distribution matrix K=(Kij)N*[log N]
Begin
F={k1,k2,….,k[log N],k1',k2',……,k'[log N]
,**for** *j = 0* **to N-1 do**
j← 0(j1,j2…….j[log N) // binary encoding
for *i=1* **to N-1do**
Assign keys from row of to user
end _

Algorithm 2: Transmission for One Traitor Case
System Server
For *ti*K*meslot* **i do**
Channel-send1=f(k(i mod[log N]),i)
@ Channel-send 2=
f(k(i mod[log N]),i)
_
Send control information on two channels
i←1
for timeslot i do
channel-listen= f(k(i mod[log N]),i)
j listens to that channel
i←i+1

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

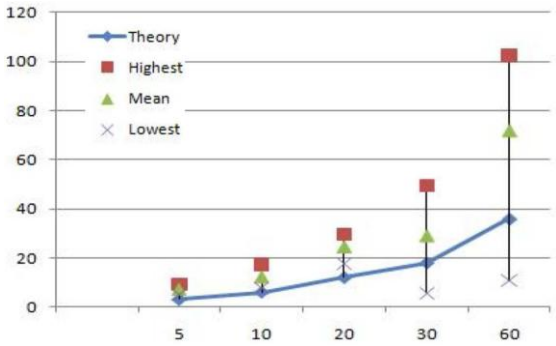


Fig 2.Detection time

VIII. RESULT ANALYSIS

Figure the influence of our constant jammer on the communication between sensor nodes. The experiment focuses on the reception of messages. In the experiment, three nodes (a jammer, a receiver, and a sender) were placed in a straight line with a distance of 10 inches from each other. The receiver was placed in the middle. We carried out 100 trials with the receiver node being under attack and another 100 trials when the jammer is replaced with a normal node sending out messages continuously to simulate the signal collision that happens frequently in benign situations. In each trial, the sender sent out 100 packets while the receiver node kept track of the number of packets received. In the figure, the X-axis represents the index of the trial and the Y-axis represents the number of times the PDR was found to have that value in the corresponding trial. Note that PDR here is the packet reception rate for a receiver node. From the figure we can see that there is a clear distinction in the number of packets a node receives with and without jamming attacks.

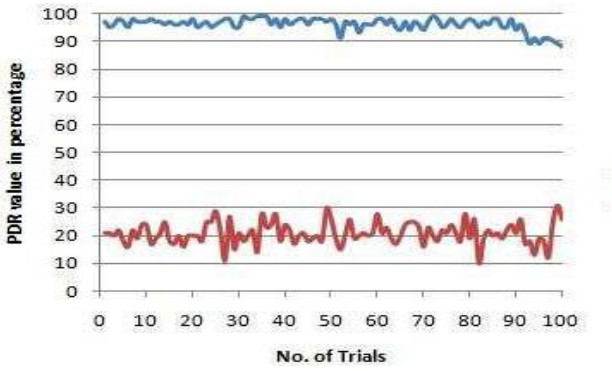


Fig 4.Performance graph

IX. CONCLUSION AND FUTURE WORK

In this paper the problem of selective jamming attacks in wireless networks has been addressed and considered an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. Showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. Evaluated the impact of selective jamming attacks on network protocols such as TCP and routing and show that a selective jammer can significantly impact performance with very low effort and developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical-layer characteristics and analyzed the security of our schemes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

and quantified their computational and communication overhead. With these schemes a random key distribution has been implemented to more secure the packet transmission in the wireless networks.

REFERENCES

1. V. Hatzivassiloglou, J.L. Klavans, M.L. Holcombe, R. Barzilay, M. Kan, and K.R. McKeown, "SIMFINDER: A Flexible Clustering Tool for Summarization," Proc. NAACL Workshop Automatic Summarization, pp. 41-49, 2001.
2. H. Zha, "Generic Summarization and Keyphrase Extraction Using Mutual Reinforcement Principle and Sentence Clustering," Proc. 25th Ann. Int'l ACM SIGIR Conf. Research and Development in Information Retrieval, pp. 113-120, 2002.
3. D.R. Radev, H. Jing, M. Stys, and D. Tam, "Centroid-Based Summarization of Multiple Documents," Information Processing and Management: An Int'l J., vol. 40, pp. 919-938, 2004.
4. R.M. Aliguyev, "A New Sentence Similarity Measure and Sentence Based Extractive Technique for Automatic Text Summarization," Expert Systems with Applications, vol. 36, pp. 7764- 7772, 2009.
5. R. Kosala and H. Blockeel, "Web Mining Research: A Survey," ACM SIGKDD Explorations Newsletter, vol. 2, no. 1, pp. 1-15, 2000.
6. G. Salton, Automatic Text Processing: The Transformation, Analysis, and Retrieval of Information by Computer. Addison-Wesley, 1989.
7. J.B MacQueen, "Some Methods for Classification and Analysis of Multivariate Observations," Proc. Fifth Berkeley Symp. Math. Statistics and Probability, pp. 281-297, 1967.
8. G. Ball and D. Hall, "A Clustering Technique for Summarizing Multivariate Data," Behavioural Science, vol. 12, pp. 153-155, 1967.
9. J.C. Dunn, "A Fuzzy Relative of the ISODATA Process and its Use in Detecting Compact Well-Separated Clusters," J.ybernetics, vol. 3, no. 3, pp. 32-57, 1973.
10. J.C. Bezdek, Pattern Recognition with Fuzzy Objective Function Algorithms. Plenum Press, 1981.
11. R.O. Duda, P.E. Hart, and D.G. Stork, Pattern Classification, second ed. John Wiley & Sons, 2001.
12. U.V. Luxburg, "A Tutorial on Spectral Clustering," Statistics and Computing, vol. 17, no. 4, pp. 395-416, 2007.
13. B.J. Frey and D. Dueck, "Clustering by Passing Messages between Data Points," Science, vol. 315, pp. 972-976, 2007.
14. S. Theodoridis and K. Koutroumbas, Pattern Recognition, fourth ed. Academic Press, 2008.
15. C.D. Manning, P. Raghavan, and H. Schu¨ tze, Introduction to Information Retrieval. Cambridge Univ. Press, 2008.

BIOGRAPHY

S.RAJASEKARAN was born on 12-05-1991 in Tamilnadu, India. He received BCA in 2011 from Muthayammal college of Arts and Science, Rasipuram, Affiliated to Periyar University, Salem, Tamilnadu, India. He received MCA in 2013 from Muthayammal College of Arts and Science, Rasipuram, Affiliated to Periyar University, Salem, Tamilnadu, India. He is Pursuing M.Phil (full time) degree from Muthayammal College of Arts & Science, in Periyar University Salem, Tamilnadu, India. His interested research area is Computer Networks.

M.GEETHA. She received her B.sc Computer Science degree from Bharathidasan University and MS(IT)., degree from Bharathidasan University.She has completed her M.Phil at Annamalai University. She is having 10 years of experience in collegiate teaching and she is the Associate Professor, Department of BCA in Muthayammal College of Arts and Science, Rasipuram affiliated by Periyar University. Her main research interests include Datamining and Warehousing.