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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Survey on Controlling Traffic with Subterfuge in Smart Gird to Minimize Message Delay under Jamming Attack

Mrs.Priyanka V. Bhagat[1], Prof. Mrs. Gayatri Bhandari[2]

M. E. Student, Dept. of Computer, JSPM's BSIOTR, Wagholi, Pune, Maharashtra, India[1]

Assistant Professor, Dept. of Information Technology, JSPM Institute of Engg &Tech, Maharashtra, India [2]

ABSTRACT: Smart grid is a cyber-physical system that integrates power infrastructures with information technologies. To facilitate efficient information exchange, wireless networks have been proposed to be widely used in the smart grid. However, the jamming attack that constantly broadcasts radio interference is a primary security threat to prevent the deployment of wireless networks in the smart grid. Hence, spread spectrum systems, which provide jamming resilience via multiple frequency and code channels, must be adapted to the smart grid for secure wireless communications, while at the same time providing latency guarantee for control messages. An open question is how to minimize message delay for timely smart grid communication under any potential jamming attack. To address this issue, we provide a paradigm shift from the case-by-case methodology, which is widely used in existing works to investigate well-adopted attack models, to the worst-case methodology, which offers delay performance guarantee for smart grid applications under any attack. We first define a generic jamming process that characterizes a wide range of existing attack models. Then, we show that in all strategies under the generic process, the worst-case message delay is a U-shaped function of network traffic load. This indicates that, interestingly, increasing a fair amount of traffic can in fact improve the worstcase delay performance.

KEYWORDS: Smart grid, wireless applications, performance modeling, worst-case analysis, message delay, jamming attacks

I. INTRODUCTION

A sensor network is an infrastructure comprised of sensing, computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. The administrator typically is a civil, governmental, commercial, or industrial entity. The environment can be the physical world, a biological system, or an information technology framework. Network sensor systems are seen by observers as an important technology that will experience major deployment in the next few years for a plethora of applications, not the least being national security. Typical applications include, but are not limited to, data collection, monitoring, surveillance, and medical telemetry. In addition to sensing, one i s often also interested in control and activation.There are four basic components in a sensor network: 1. An assembly of distributed and localized sensors; 2. An interconnecting network; 3. A central point of information clustering; and 4. A set of computing resources at the central point to handle data correlation, event trending, status querying, and data mining.

The smart grid is an emerging cyber-physical system that incorporates networked control mechanisms (e.g, advanced metering and demand response) into conventional power infrastructures. To facilitate information delivery for such mechanisms, wireless networks that provide flexible and un- tethered network access have been proposed and designed for a variety of smart grid applications. However, the use of wireless networks introduces potential security vulnerabilities due to the shared nature of wireless channels. It has been pointed out in that the jamming attack, which uses radio interference to disrupt wireless communications can result in network performance degradation and even denial-of-service in power applications, thereby being a primary security threat to prevent the deployment of wireless networks for the smart grid. How to defend against jamming attacks is of critical importance to secure wireless communications in the smart grid. There have been extensive works on designing spread spectrum based

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

communication schemes, which provide jamming resilience by using multiple orthogonal frequency or code channels. Interesting enough, most efforts attempt to design point-to-point or broadcast schemes such that a message can be sent to its destination. However, the key question to jamming-resilient communication for the smart grid is not whether a message can finally reach its destination, but whether it can be successfully delivered on time for time- critical power applications. For example, substation mess ages have 3ms–500ms delay constraints for reliable operation. The over-due delivery of such messages directly results in communication failure, and can potentially lead to system instability. Therefore, an open question in the smart grid is how to minimize message delay in spread spectrum based wireless networks under jamming attacks. In this paper, we address this issue by considering a wireless network that uses multiple frequency and code channels to provide jamming resilience for time-critical smart grid applications. As message delivery in the smart grid becomes invalid as long as its delay D is greater than the delay threshold σ our goal is to minimize the message invalidation probability P (D>σ) in the presence of jamming attacks. A key observation in our approach is that there are two opposites in the network: the network operator and jammer attempt to minimize and maximize P (D>σ), respectively. As a result, we adopt a min- max approach to study the problem: i) find out which jamming attack can maximize P (D>σ) (e.g. the worst-case attack), ii) given the worst-case attack, attempt to minimize P (D>σ).

II. RELATED WORK

In this section we survey on different papers related to the wireless application, attacks. In [5], Li et al have considered controllable jamming attacks that are not difficult to dispatch and hard to detect and stand up to, since they vary from brute force attacks. The jammer controls probability of jamming and transmission go to cause maximal harm to the network as far as adulterated communication links. They have especially helped; (i) determined the ideal assault and protection systems as answers for advancement issues that are confronted by the aggressor and the network individually by incorporating in the detailing vitality restrictions, (ii) for assault detection, gave an ideal detection test that determines choices focused around the measurable rate of brought about crashes, (iii) included in the definition assault detection and exchange of the assault warning message out of the jammed region.

There are different impedances or issues on immediate sequence spread spectrum communication channel particularly jamming issues, so as to concentrate on this issue an immediate sequence spread spectrum (DSSS) communication framework utilizing Gold code was utilized as point -to-point with completely synchronized in the middle of transmitter and collector under the impact of Additive White Gaussian Noise (AWGN) channel and single tone jamming (STJ) and multi tone jamming (MTJ) [8].

C. Popper et al [2] concentrated on a related however distinctive issue for broadcast communication: How to empower robust against jamming broadcast without shared secret keys? As an answer for the portrayed issue, we propose a plan called Uncoordinated DSSS (UDSSS) that empowers authentic spread-spectrum against jamming broadcast without the prerequisite of shared secrets. UDSSS keeps unscrupulous collectors from meddling with the communication (to different recipients) while it empowers them to get the data themselves.After a certain time, each beneficiary will succeed in distinguishing the right spreading code and its synchronization, along these lines dispreading the sign.

M Strasser et al [9] address and depict the opposition to jamming/key establishment circular dependency issue: against jamming spread spectrum communication procedures depend on a shared (spreading) key and key establishment depends on a jamming-safe communication. As one answer for the tended to issue, they have proposed a plan called UFH (Uncoordinated Frequency Hopping) that empowers two nodes to execute a key establishment protocol in the vicinity of a jammer; the made key can then be utilized to help later coordinated frequency hopping communication. The UFH plan underpins the transmission of messages of subjective length in a jammed environment without depending on a shared secret key.

III. PROPOSED ALGORITHM

TACT measures the delivery results of probing messages to adjust the amount of camouflage messages in the network. Each camouflage message is transmitted on a randomly selected frequency/code channel. When TACT is deployed, there are three major traffic types in the network: i) routine traffic for power monitoring and control, which cannot be

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

changed as it is coupled with setups of power devices, ii) probing traffic for performance measurement, its message transmission time equals to TL, iii) camouflage traffic to balance the overall network traffic load. The first observation period, two probing messages are both ACKed, meaning that current traffic load is not harmful. Then, TACT sends one more camouflage message in the next observation period. The traffic load will keep being increased until it reaches the optimum, and finally fluctuate around the optimum.

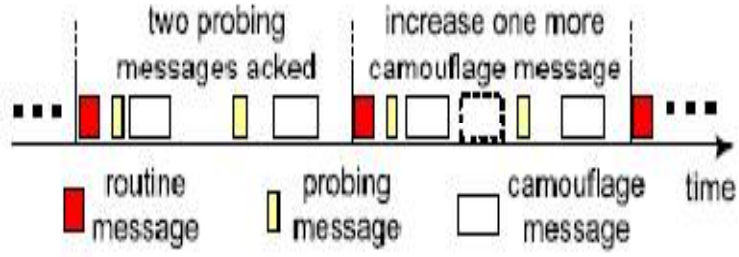

Figure 1. How TACT balances the network traffic.

1) Algorithm 1:

TACT At Each Node :
Given : L, Lmin, Lmax, ▲inc,▲dec,
Init : Mprev = 0
L = Lmin: repeat transmit probing messages in observation period.
measure the number ofACks, Mnow
if performance not degraded (Mnow > Mprev)then
Increase the traffic load:L ←min(L +4inc;Lmax) else
decrease the traffic load:L ←max(L -▲dec;Lmin):
else if
record history: Mprev ←Mnow
until TACT is disable

TACT in Coordinated and Uncoordinated Modes: So far, we have presented the fundamentals of TACT to minimize the worst-case message delay under jamming attacks. Although we have shown that uncoordinated w communication is not appropriate for time-critical applications, it is still essential to establish the secret key for coordinated communication. As a result, both communication modes are indispensable to fully secure communications for time-critical applications in the smart grid. Specifically, uncoordinated mode is used for key establishment and update. After the secret key is established or updated, the two communicators can use coordinated mode to exchange information based on the secret key. Hence, to substantially improve the performance of a wireless smart grid application with jamming resilience, TACT should be adapted to both coordinated and uncoordinated communications. This means that TACT must be enabled as long as a node is active, regardless of the mode on which it operates. Accordingly, we summarize the complete jamming-resilient communication scheme with TACT in Algorithm 2.

2) Algorithm 2:

Communication Schema with TACT:
Init: Enable TACT
repeat
Mode←UncoordinatedMode
Obtain Key K and period Tk form gateway
Mode←Coordinatedmode

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Use K for a Period of Tk until The node leaves the network

IV. SYSTEM ARCHITECTURE

In Proposed system, to where about the problem of message delay under jamming by considering wireless network that take number of frequency and channels to supply jamming resilience for smart grid application. In this system consider two general jamming-resilience communications for smart grid application first is coordinated modes another is uncoordinated modes.Coordinated communication is a conventional model in spectrum systems.Using uncoordinated communication establish an initial key. In uncoordinated communication,the sender and receiver randomly elect a frequency-code channel totransmit and receive, respectively.A message can be delivered from sender to receiver when they both reside at the same channel. We define a generic jamming process to find out the worst-case attack .Then we show that theoretical analysis .Performance show that camouflage traffic can decrease the message disannual chance in order of magnitude, and thus it is a promising elimination to battle reactive jamming for smart grid applications.

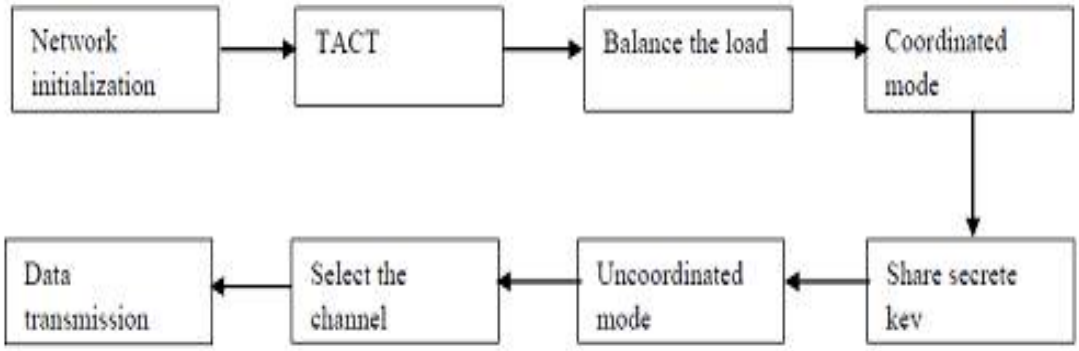

Figure 2: System Architecture

Implementation Of Jamming Attack In Wireless Networks: In implementation of jamming attack in wireless networks module, a wireless network is created. All the nodes are configured and randomly deployed in the network area. Since our network is a wireless network, nodes are assigned with mobility (movement). A routing protocol is implemented in the network. Sender and receiver nodes are randomly selected and the communication is initiated. A node is configured as jamming node so as to send data packets with abnormal rate and disrupt the network activity. Performance Analysis: In performance analysis module, the performance of the network under the presence of jamming node is analyzed. Based on the analyzed results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters are considered here and X-graphs are plotted for these parameters. Detection of Jamming Using TACT: According to this method, TACT transmits camouflage traffic packets to balance the overall network traffic load. TACT considers two general jamming-resilient communication modes for smart grid applications: Coordinated mode and uncoordinated mode. In coordinated mode, the sender and receiver share a common secret or key (e.g., code-frequency channel assignment), which is unknown to attackers. In uncoordinated communication, the sender and receiver randomly choose a frequency-code channel to transmit and receive, respectively. Performance Analysis: In performance analysis module, the performance of the proposed TACT method is analysed. Based on the analysed results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters considered here and X-graphs are plotted for these parameters. Finally, the results obtained from this module is compared with previous results and comparison X-graphs are plotted.

V. CONCLUSION AND FUTURE WORK

To design a distributed method, at optimal point generate camouflage traffic to balance the network load. This paper shows that TACT is good method to improve the delay performance in smart grid under jamming attacks. We have shown that uncoordinated communication is not right for time-critical applications; it is stable basic to found the secret

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

key for coordinated communication.as a output, both communication modes are indispensable to fully secure communication for time-critical application in smart grid. Particularly uncoordinated mode is used for establishment and update. After the secrete key established or updated, the communicators can use coordinated mode to exchange information based on the secret key. Hence the performance ofa wireless smart grid application with jamming resilience. Accordingly,we summarize the complete jamming-resilient communication scheme with TACT.

REFERENCES

[1] Zhuo Lu, Wenye Wang, Cliff Wang, Camouflage Traffic: MinimizingMessage Delay for Smart Grid Applications under Jamming ,in proc.IEEE transactions on dependable and secure computing, vol. 12, no. 1,January/February 2015.
[2] Akyol .B, Kirkham .H, Clements .S, and Hadley .M, A survey of wirelesscommunications for the electric power system, in Tech. Rep., Richland, WA, USA, Pacific Northwest Nat. Laboratory,PNNL-19084, Jan. 2010.
[3] Bayraktaroglu .E, King .C, Liu .X, Noubir .G, Rajaraman .R, and Thapa.B, On the performance of IEEE 802.11 under jamming, in Proc. IEEE IEEE Conf. Comput. Commun., pp. 12651273, Apr. 2008.
[4] Brinkmeier .M, Schafer .G, and Strufe .T, Optimally DoS resistant P2Ptopologies for live multimedia streaming, IEEE Trans. Parallel Distrib Syst., vol. 20, no. 6, pp. 831844, Jun. 2009.
[5] Cleveland .F, Uses of wireless communications to enhance power systemreliability, in Proc. IEEE Power Eng. Soc. Gen. Meeting, p. 1, Jun. 2007.
[6] El-Khattam .W, Sidhu .T .S, and Seethapathy .R, Evaluation of two antiislandingschemes for a radial distribution system equipped with selfexcitedinduction generator wind turbines,
[7] Guidelines for Smart Grid Cyber Security, NIST IR-7628, NIST SmartGrid Cyber Security Working Group, vol. 1-3, Aug. 2010.
[8] Li .H, Lai .L, and Qiu .R .C, A denial-of-service jamming game forremote state monitoring in smart grid, in Proc. 45th Annu. Conf. Inf. Sci. Syst., pp. 16, Mar. 2011.
[9] B. Akyol, H. Kirkham, S. Clements, and M. Hadley, A survey of wirelesscommunications for the electric power system, Pacific Northwest NationalLab., Richland, WA, USA, Tech. Rep. PNNL-19084, Jan. 2010.
[10] C. Popper, M. Strasser, and S. Capkun, Jamming resistant broadcastcommunication without shared keys, in Proc. USENIX Security, Berkeley, CA, USA, Aug. 2009.
[11] M. Li, I. Koutsopoulos, and R. Poovendran, Optimal jamming attacksand network defense policies in wireless sensor networks, in Proc. IEEE INFOCOM, May 2007, pp. 13071315
[12] W. Xu, W. Trappe, Y. Zhang, and T. Wood, The feasibility of launchingand detecting jamming attacks in wireless networks, in Proc. ACM MobiHoc, Urbana-Champaign, IL, USA, 2005, pp. 4657.
[13] X. Lu, Z. Lu, W. Wang, and J. Ma, On network performance evaluationtoward the smart grid: A case study of DNP3 over TCP/IP, in Proc. IEEEGLOBECOM, Houston, TX, USA, Dec. 2011

BIOGRAPHY

Mrs.Priyanka V. Bhagat is ME, Student at Computer Dept. JSPM Institute of Engg &Tech, Pune, Maharashtra, India.

Prof. Mrs. Gayatri Bhandari is an Assistant Professor at, Department of Computer Engineering,JSPM Institute of Engg &Tech,Pune, Maharashtra, India.