# "Primary security threat to prevent the deployment of wireless networks in the smart grid"

NEHA V. HARDE [1] Prof.MIRZA M. BAIG[2]

*DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING*
*J D COLLEGE OF ENGINEERING AND MANAGEMENT*
*NAGPUR, MAHARASHTRA, INDIA*

## ABSTRACT

*The Smart Grid, generally referred to as the next-generation power system, is considered as a revolutionary and evolutionary regime of existing power grids. More importantly, with the integration of advanced computing and communication technologies, the Smart Grid is expected to greatly enhance efficiency and reliability of future power systems with renewable energy resources, as well as distributed intelligence and demand response. Along with the silent features of the Smart Grid, cyber security emerges to be a critical issue because millions of electronic devices are inter-connected via communication networks throughout critical power facilities, which has an immediate impact on reliability of such a widespread infrastructure. We present a comprehensive survey of cyber security issues for the Smart Grid. Specifically we focus on reviewing and discussing security requirements, network vulnerabilities, attack countermeasures, secure communication protocols and architectures in the Smart Grid. Aim to provide a deep understanding of security vulnerabilities and solutions in the Smart Grid and shed light on future research directions for Smart Grid security.*

**Keywords** —*Jamming, security, jamming detection and mitigation, optimization, wireless sensor network, advanced metering infrastructure (AMI), Smart Grid, Message Delay, RC4.*

## 1. Introduction

In past decades, the development of power grids has not been keeping pace with the industrial and social advancements that drastically increase the demand on power supply. For example, statistics showed that from 1950 to 2008, energy production and consumption in the US increase approximately two and three times, respectively. In particular, the public/commercial services, industry and residential areas are the most demanding areas for electricity in theUS in 2008. In order to cope with such a demand increase, one major challenge is to efficiently manage a variety of energy resources, including traditional fossil fuel sources (e.g., coal, petroleum, and natural gas), and renewable energy resources (e.g., solar and hydro) . Therefore, the National Institute of Standards and Technology (NIST) rolled out national efforts to develop the next-generation electric power system, commonly referred to as the Smart Grid. Compared with legacy power systems,

The Smart Grid is envisioned to fully integrate high-speed and two-way communication technologies into millions of power equipment's to establish a dynamic and interactive infrastructure with new energy management capabilities, such as advanced metering infrastructure (AMI) and demand response. However, such a heavy dependence on information networking inevitably surrenders the Smart Grid to potential vulnerabilities associated with communications and networking systems. This in fact increases the risk of compromising reliable and secure power system operation. For example, it has been shown that potential network intrusion by adversaries may lead to a variety of severe consequences in the Smart Grid, from customer information leakage to a cascade of failures, such as massive blackout and destruction of infrastructures.

As a result, weare trying to investigate cyber security issues in the Smart Grid, which is of critical importance to the design of information networks and has been considered as one of the highest priorities for the Smart Grid design. Since the research on cyber security for the Smart Grid is still in its early stage, our objective is to provide an overview, analyze potential cyber security threats, review existing security solutions, and summarize research challenges in the Smart Grid.

## 2. LITERATURE REVIEW

The numbers of researches were presented by the different researcher for analysis of Primary security threat to prevent the deployment of wireless networks in the smart grid are as follows:

**2.1ZhuoLu [1].**Has been studied on the 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, they 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. They 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 worst-case delay performance. As a result, they demonstrate a lightweight yet promising system, TACT (transmitting adaptive camouflage traffic), to combat jamming attacks. TACT minimizes the message delay by generating extra traffic called camouflage to balance the network load at the optimum. Experiments show that TACT can decrease the probability that a message is not delivered on time in order of magnitude.

**2.2 Akyol .B, Kirkham [2]** has been studied on Wireless communications provide both flexibility and cost savings in deployment and maintenance compared to wireline deployments. Wireless can be deployed anywhere and anytime. No trenches or conduits are required. Wireless networks using mesh technology such as Wireless HART can route around not only single but also multiple node failures. Sensors that use IEEE 802.15.4 based radio transceivers (e.g., ISA100.11a) can function for several years with an internal battery in harsh environments without requiring any external power. A sensor that has wireless capabilities can be easily relocated and when required, additional supplementary sensors can be deployed in most cases within a few hours. To summarize, with wireless communications we gain ease of deployment, flexibility, and cost savings. Common challenges associated with wireless communications are probabilistic channel behavior, accidental and directed interference or jamming, and eavesdropping or unauthorized modification of the communications if not protected by authentication and encryption. A wireless communication network without proper security protocols can be exploited with a man-in-the-middle attack. The result could be both loss of service and loss of confidentiality. Wireless-based systems have been used in industries similar to the electric power system such as oil and gas.

**2.3 Bayraktaroglu .E [3]**Hasbeen studiedthe performance of the IEEE 802.11 MAC protocol under a range of jammers that covers both channel-oblivious and channel-aware jamming. They 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. they 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, they measure the real-world performance of periodic and memory less jammers using our GNU radio jammer prototype.

**2.4Brinkmeier .M[4]**Has been studied on peer-to-peer approach for live multimedia streaming applications offers the promise to obtain a highly scalable, decentralized, and robust distribution service. When constructing streaming topologies, however, specific care has to be taken in order to ensure that quality of service requirements in terms of delay, jitter, packet loss, and stability against deliberate denial of service attacks are met. In this paper, we concentrate on the latter requirement of stability against denial-of-service attacks. They present an analytical model to assess the stability of overlay streaming topologies and describe attack strategies.

Building on this, we describe topologies, which are optimally stable toward perfect attacks based on global knowledge, and give a mathematical proof of their optimality. The formal construction and analysis of these topologies using global knowledge lead us to strategies for distributed procedures, which are able to construct resilient topologies in scenarios, where global knowledge cannot be gathered. Experimental results show that the topologies created in such a real-world scenario are close to optimally stable toward perfect denial of service attacks.

**2.5 Cleveland .F[5]**Has been studied on Wireless data communications, such as WiFi, cellular systems, and meshed wireless networks, are being assessed by many industries, since they can offer significant "bottom line" benefits over wired communications. These benefits include low cost installations, rapid deployment, easy user access, mobility, and feasibility of functions not possible or not economically feasible with wired communications. Given these benefits, additional condition monitoring, safety monitoring, security management, and other new functions can be added to the arsenal for enhancing power system reliability.

**2.6 MingyanLi [6]**Has been studied on a sophisticated jammer jams an area in which a single-channel random-access-based wireless sensor network operates. The jammer controls the probability of jamming and the transmission range in order to cause maximal damage to the network in terms of corrupted communication links. The jammer action ceases when it is detected by the network (namely by a monitoring node), and a notification message is transferred out of the jammed region. The jammer is detected by employing an optimal detection test based on the percentage of incurred collisions. On the other hand, the network defends itself by computing the channel access probability to minimize the jamming detection plus notification time. The necessary knowledge of the jammer in order to optimize its benefit consists of knowledge about the network channel access probability and the number of neighbors of the monitor node. Accordingly, the network needs to know the jamming probability of the jammer. they study the idealized case of perfect knowledge by both the jammer and the network about the strategy of each other and the case where the jammer and the network lack this knowledge. The latter is captured by formulating and solving optimization problems where the attacker and the network respond optimally to the worst-case or the average-case strategies of the other party. they also take into account potential energy constraints of the jammer and the network. We extend the problem to the case of multiple observers and adaptable jamming transmission range and propose a meaningful heuristic algorithm for an efficient jamming strategy. Our results provide valuable insights about the structure of the jamming problem and associated defense mechanisms and demonstrate the impact of knowledge as well as adoption of sophisticated strategies on achieving desirable performance.

**2.7 J.oburadha[7]** Has been studied on Wireless sensor networks are network that consists of sensors which are distributed in an adhoc manner. These sensors work with each other to sense some physical phenomenon and then the information gathered is processed to get relevant results. Wireless sensor consists of protocols and algorithms. The basic components of sensor nodes are sensing unit, processing unit, trans-receiver, and power unit. Smart grid is a digital physical framework that Incorporates power foundations with data innovations.It prevents the data from message delay and jamming and it secures the encrypted data.

**2.8 Ping Yia[8]**Has been studied on Advanced Metering Infrastructure (AMI) is the core component in a smart grid that exhibits a highly complex network configuration. AMI shares information about consumption, outages, and electricity rates reliably and efficiently by bidirectional communication between smart meters and utilities. However, the numerous smart meters being connected through mesh networks open new opportunities for attackers to interfere with communications and compromise utilities assets or steal customers private information.

In this paper, they present a new DoS attack, called puppet attack, which can result in denial of service in AMI network. The intruder can select any normal node as a puppet node and send attack packets to this puppet node. When the puppet node receives these attack packets, this node will be controlled by the attacker and flood more packets so as to exhaust the network communication bandwidth and node energy. Simulation results show that puppet attack is a serious and packet deliver rate goes down to 20–10%. After analyzing the puppet attack, they propose the detection and prevention mechanism. Simulations show that puppet attack causes the same damage as a flooding attack and the proposed method can prevent the puppet attack efficiently.

**2.9 YakubuTsado[9]**has been studied on Smart grid combines a set of functionalities that can only be achieved through ubiquitous sensing and communication across the electrical grid. The communication infrastructure must be able to cope with an increasing number of traffic types which is as a result of increased control and monitoring, penetration of renewable energy sources and adoption of electric vehicles. The communication infrastructure must serve as a substrate that supports different traffic requirements such as QoS (i.e. latency,

bandwidth and delay) across an integrated communication system. This engenders the implementation of middleware systems which considers QoS requirements for different types of traffic in order to allow prompt delivery of these traffic in a smart grid system. A heterogeneous communication applied through the adaptation of the Ubiquitous Sensor Network (USN) layered structure to smart grid has been proposed by the International Telecommunication Union (ITU). This paper explores the ITU's USN architecture and presents the communication technologies which can be deployed within the USN schematic layers for a secure and resilient communication together with a study of their pro's and con's, vulnerabilities and challenges. It also discusses the factors that can affect the selection of communication technologies and suggests possible communications technologies at different USN layers. Furthermore, the paper highlights the USN middleware system as an important mechanism to tackle scalability and interoperability problems as well as shield the communication complexities and heterogeneity of smart grid.

**2.10 Hongbo Liu [10]** has been studied on a key component of a smart grid is its ability to collect useful information from a power grid for enabling control centers to estimate the current states of the power grid. Such information can be delivered to the control centers via wireless or wired networks. They envision that wireless technology will bewidely used for local-area communication subsystems in the smart grid (e.g., in distribution networks). However, various attacks with drastic impacts can be launched in wireless networks such as channel jamming attacks and DoS attacks. In particular, jamming attacks can cause a wide range of damages to power grids, e.g.,delayed delivery of time-critical messages can prevent control centers from properly controlling the outputs of generators to match load demands. In this paper, they design a communication subsystem with enhanced self-healing capability under the presence of jamming through intelligent local controller switching. Our proposed framework allows sufficient readings from smart meters to be continuously collected by various local controllers to estimate the states of a power grid under various attack scenarios. In addition, they provide guidelines on optimal placement of local controllers to ensure effective switching of smart meters under jamming. Via theoretical, experimental and simulation studies, they demonstrate that our proposed system is effective in maintaining communications between smart meters and local controllers even when multiple jammers are present in the network.

**Proposed system**

In proposed system, to address the issue of message delay under jamming by considering a wireless network that uses multiple frequency and code channels to provide jamming resilience for smart grid applications. In this system consider two general jamming-resilient communication modes for smart grid applications: coordinated and uncoordinated modes. Coordinated communication is a conventional model in spread spectrum systems. However, the transmitter and receiver may not share a common secret initially e.g., a node joins a network and attempts to establish a secret with others. Uncoordinated communication is therefore used to help establish such an initial key. In uncoordinated communication, the sender and receiver randomly choose a frequency-code channel to transmit and receive, respectively. A message can be delivered from the sender to the receiver only if they both reside at the same channel, and at the same time the jammer does not disrupt the transmission on the channel. By defining a generic jamming process, we can show that the worst-case message delay is a U-shaped function of network traffic load. To designed a distributed method, TACT, to generate camouflage traffic to balance the network load at the optimal point. This showed that TACT is a promising method to significantly improve the delay performance in the smart grid under jamming attacks. Minimization of the network overload. Message delay among the network is made low. Performance of the system is increased.

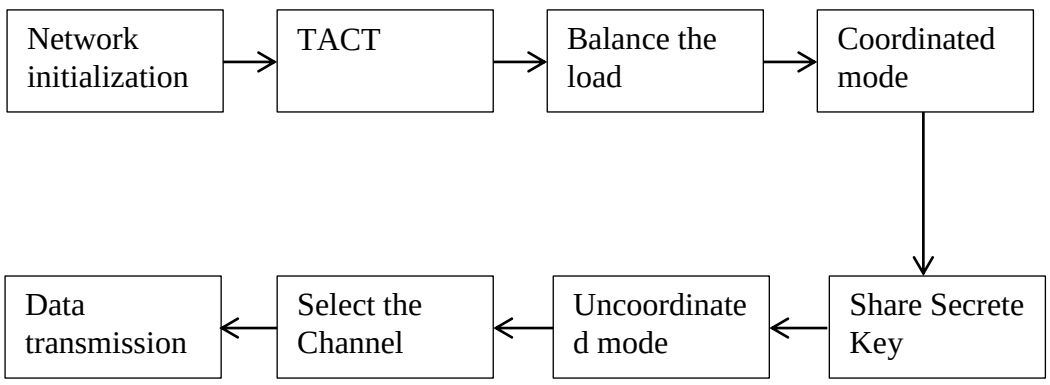


Fig.1 System Architecture

## 3. Conclusion

As a result, this paper present both communication modes are indispensable to fully secure communications fortime-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 the solutions enhance overall network functionality while simultaneously making security easier and less costly to manage.

## 4. Future Scope

In this paper, we provide a study on minimizing the message delay for smart grid applications under overcrowding attacks. By defining a generic overcrowding process, we showed that the worst-case message delay is a U-shaped function of network traffic load. Thus, we show that generating camouflage traffic is a promising method to improve the worst-case delay performance in the smart grid under overcrowding attacks. Maximum avoided traffic overcrowding delay.

Solution for preventing the various kind of attack in the system those that happen in this software.

## 5. References


[1] Zhuo Lu, Wenye Wang, Cliff Wang," Camouflage Traffic: Minimizing Message Delay for Smart GridApplications 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 wireless communications for theelectric 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 ofIEEE 802.11 under jamming," in Proc. IEEE Conf. Comput. Commun., pp. 1265–1273, Apr. 2008.

[4] Brinkmeier .M, Schafer .G, and Strufe .T, "Optimally DoS resistant P2P topologies for live multimediaStreaming," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 6, pp. 831–844, Jun. 2009.

[5] Cleveland .F, "Uses of wireless communications to enhance power system reliability," in Proc. IEEEPower Eng. Soc. Gen. Meeting, p. 1, Jun. 2007.

[6] Mingyan. Li, I. Koutsopoulos, and R. Poovendran, "Optimal Jamming Attacks and Defense Policies in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2007.

[7] J.oburadha, "Controlling traffic in smart grid application"International Conference on Explorations and Innovations in Enginering&Technol,ICEIET-2016

[8] Ping Yia, , Ting Zhub, QingquanZhangb, YueWua "A denial of service attack in advanced metering infrastructure network " Volume 59, January 2016, Pages 325–332

[9] YakubuTsado, David Lund, Kelum A.A. Gamage "Resilient communication for smart grid ubiquitous sensor network" Computer Communications, Volume 71, 1 November 2015.

[10] Hongbo Liu, Yingying Chen "Towards Self-Healing Smart Grid via Intelligent

[11] Local Controller Switching under Jamming "in IEEE conference on computer network & security 2013.