International Journal of Computer Science and Engineering Communications,
Volume.4, Issue.2 (2016): Page.1393-1396
www.scientistlink.com/ijcsec

# Adaptive Packet Transmission in Smart Grid to Minimize the Message Delay

**K.Suganya*, A.Mummoorthy****
**PG Scholar,** Assistant Professor,*
*Department of Computer Science,*
*K.S.R.College of Engineering, India*
*suganyaakanagaraj@gmail.com,amummoorthy@gmail.com*

***Abstract:*** *Smart grid is a digital physical framework that incorporates power foundations with data innovations. To encourage proficient data trade, remote systems have been proposed to be broadly utilized as a part of the shrewd framework. In any case, the sticking assault that always telecasts radio obstruction is an essential security risk to keep the sending of remote systems in the keen network. Consequently, spread range frameworks, which give sticking versatility by means of numerous recurrence and code channels, must be adjusted to the keen network for secure remote correspondences, while in the meantime giving idleness surety to control messages. An open inquiry is the manner by which to minimize message delay for convenient savvy lattice correspondence under any potential sticking assault. To address this issue, we give a standard transformation from the case-by-case philosophy, which is generally utilized as a part of existing attempts to examine all around received assault models, to the most pessimistic scenario approach, which offers delay execution ensure for keen framework applications under any assault. At that point, we demonstrate that in all methodologies under the non specific process, the most pessimistic scenario message postponement is a U-formed capacity of system activity load. This demonstrates that, interestingly, expanding a decent measure of movement can truth be told enhance the worstcase delay execution. Accordingly, we show a lightweight yet encouraging framework, transmitting versatile disguise movement , to battle sticking assaults. Judgment minimizes the message delay by creating additional movement called cover to adjust the system load at the ideal. Trials demonstrate that TACT can diminish the likelihood that a message is not conveyed on time all together of extent.*

***Keywords:*** *Smart Grid, Message Delay, Worstcase Delay, TACT.*

## 1. 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 is 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.

## 2. RELATED WORK

Zhuo Lo proposed the problem of Problem-sender should not analysis about attackers and traffic. Technique used here isTACT(Transmitting Adaptive camouflage traffic). Zhenhua Liu proposed the problem of Indirect measurements affected by jamming attacks. Heuristic search algorithm, Error minimizing based search algorithm are the techniques. Guevara Noubir proposed the problem Block the source node during the transaction by the attacker. Nash equilibrium is the technique used. In this paper Fail to provide a guaranteed reliable Network. Velocity Energy Efficient And Link Aware Cluster-Tree(VELCT) is used to recover the problem.

## 3. JAMMING ATTACKS

Wireless technologies have become increasingly popular in our everyday business and personal lives. It enables one or more devices to communicate without physical connections without requiring network or peripheral cabling. As we know that wireless networks serve as the transport mechanism between devices and among devices. However, because of this wireless nature these are prone to multiple security threats in which one of the major serious security threat is jamming. Jamming can disrupt wireless transmission and can occur either unintentionally in the form of noise or interference at the receiver side. Jamming attacks may be viewed as a special case of Denial of service attack. In simplest form of jamming, the attacker interferes with the set of frequency bands used for communication by transmitting a continuous jamming signal or several short jamming pulses. Normally Jamming attacks have been considered under an external threat model, but here we are considering jamming attacks under an internal threat model. Under an external threat model, jamming strategies transmits high power interference signals continuously or randomly. This type of strategies has several disadvantages. First, the attacker has to spend huge amount of energy in order to jam certain frequency bands. Second, these types of attacks are easy to detect because of continuous presence of unusually high interference levels. A well-known countermeasure against this type of jamming attacks are spread spectrum techniques such jamming is referred as jamming gain.

### 1.3.1 CONSTANT JAMMER

The constant jammer continually emits a radio signal. It has implemented a constant jammer using two types of devices. The first type of device to use is a waveform generator which continuously sends a radio signal. The second type of device it used is a normal wireless device. In this author, it will focus on the second type, which it built on the MICA2 Mote platform. This constant jammer continuously sends out random bits to the channel without following any MAC layer etiquette. Specifically, the constant jammer does not wait for the channel to become idle before transmitting. If the underlying MAC protocol determines whether a channel is idle or not by comparing the signal strength measurement with a fixed threshold.

### 1.3.2 DECEPTIVE JAMMER

Instead of sending out random bits, the deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions. As a result, a normal communicator will be received into believing there is a legitimate packet and will be duped to remain in the receive state. For example, in Tiny OS, if a preamble is detected, a node remains in the receive mode, regardless of whether that node has a packet to send or not. Hence, even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected. Further, it also observes that it is adequate for the jammer to only send a continuous stream of preamble bits rather than entire packets.

### 1.3.3 RANDOM JAMMER

Instead of sending out a radio signal continuously, a random jammer alternates between sleeping and jamming. Specifically, after jamming for tj units of time, it turns on its radio, and enters a sleeping mode. It will resume jamming after sleeping for ts time. tj and ts can be either random or fixed values. During its jamming phase, it can either behave like a constant jammer or a deceptive jammer. Throughout this art hour, this random jammer will operate as a constant jammer during jamming. The distinction between this model and the previous two models lies in the fact that this model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply. By adjusting the distribution governing the values of tj and ts, it can achieve various levels of trade-off between energy efficiency and jamming effectiveness.

### 1.3.4 REACTIVE JAMMER

The three models discussed above are active jammers in the sense that they try to block the channel irrespective of the traffic pattern on the channel. Active jammers are usually effective because they keep the channel busy all the time. These methods are relatively easy to detect. An alternative approach to jamming wireless communication is to employ a reactive strategy. For the reactive jammer, it takes the view point that it is not necessary to jam the channel when nobody is communicating. Instead, the jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. As a result, a reactive jammer targets the reception of a message. It would like to point out

that a reactive jammer does not necessarily conserve energy because the jammer's radio must continuously be on in order to sense the channel. The primary advantage for a reactive jammer, however, is that it may be harder to detect.

## 4. EXISTING SYSTEMS

Smart grid is an emerging cyber-physical system that incorporates networked control mechanisms into conventional power infrastructures. The use of wireless networks introduces potential security vulnerabilities due to the shared nature of wireless channels. The NIST has recently imposed a strong requirement for smart grid security: power system operations must be able to continue during any security attack or compromise. This means that the widely-used case-by-case methodology cannot be readily adapted to wireless smart grid applications, because it is not able to guarantee reliable communication under any potential jamming attack. To provide such a guarantee, securing wireless smart grid applications requires a paradigm shift from the case-by-case methodology to a new worst-case methodology that offers performance assurance under any attack scenario. On the other hand, it has been shown that the message delay performance can be substantially worsen and even violate the timing requirement of control applications under inappropriate security design. The message delay can happen for timely smart grid communication under any potential jamming attack. By using this method we only minimizing the message delay on wireless communication system. It is partially reduce the delay performance in the smart grid under jamming attacks due to the worse case method's weak security these are all the drawbacks of the existing system.

## 5. 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.

## 6. MODULES

### 6.1 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.

### 6.2 Performance Analysis

In performance analysis module, the performance of the network under the presence of jamming node is analysed. Based on the analysed results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters are considered here and X-graphs are plotted for these parameters.

### 6.3 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.

**6.4 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. Form the comparison result, final RESULT is concluded.

## 7. CONCLUSION

In this paper, we provided a comprehensive study on minimizing the message delay for smart grid applications under jamming attacks. By defining a generic jamming process, it showed 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 paper showed that TACT is a promising method to significantly improves the delay performance in the smart grid 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.

## REFERENCES

[1] Zhuo Lu, Wenye Wang, Cliff Wang," Camouflage Traffic: Minimizing Message 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 wireless communications 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. 1265–1273, Apr. 2008.

[4] Brinkmeier .M, Schafer .G, and Strufe .T, "Optimally DoS resistant P2P topologies for live multimedia streaming," 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. IEEE Power Eng. Soc. Gen. Meeting, p. 1, Jun. 2007.

[6] El-Khattam .W, Sidhu .T .S, and Seethapathy .R, "Evaluation of two anti-islanding schemes for a radial distribution system equipped with self-excited induction generator wind turbines,"

[7] Guidelines for Smart Grid Cyber Security, NIST IR-7628, NIST Smart Grid Cyber Security Working Group, vol. 1-3, Aug. 2010.

[8] Li .H, Lai .L, and Qiu .R .C, "A denial-of-service jamming game for remote state monitoring in smart grid," in Proc. 45th Annu. Conf. Inf. Sci. Syst., pp. 1–6, Mar. 2011.

[9] Liu .Y, Ning .P, Dai .H, and Liu .A, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in Proc. IEEE IEEE Conf. Comput. Commun., pp. 1–9. Mar. 2010.