International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2763
Issue 04, Volume 3 (April 2016) SPECIAL ISSUE www.ijirae.com

# CONTROLLING TRAFFIC IN SMART GRID APPLICATION

**J.Oburadha**
*PG Student*
*Department of CSE*
*Sengunthar College of Engineering*

**K.Sudhakar**
*Assistant Professor*
*Department of CSE*
*Sengunthar College of Engineering*

***Abstract- 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, transreceiver, and power unit. Smart grid is a digital physical framework that incorporates power foundations with data innovations. The jamming attack that constantly broadcasts radio interference is a primary security threat to prevent the deployment of wireless networks in the smart grid. In this paper, we are preventing the jamming attack by using RC4 algorithm. It prevents the data from message delay and jamming and it secures the encrypted data.***

***Keywords - Smart Grid, Message Delay, Jamming, RC4***

## 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 components of a wireless sensor network enable wireless connectivity within the network, connecting an application platform at one end of the network with one or more sensor or actuator devices in any part of the network. The characteristics of wireless sensor nodes are power consumption constraints for nodes using batteries or energy harvesting. Ability to cope with node failures modes of mobility, heterogeneity of nodes.

## 2. RELATED WORK

An efficient cluster- tree based data collection scheme for large mobile wireless sensor networks, in this paper the main problem is time delay and not guaranteed reliable network. So by using the velocity energy- efficient and link aware cluster-tree form the cluster head for decrease the time delay. A secure scheme against power exhausting attacks in hierarchical wireless sensor network, in this paper the main problem is denial of sleep attack shorten the lifetime of wireless sensor network and MAC protocol are insufficient to protect the WSN from denial of sleep attack. To overcome this problem secure adaptive topology control algorithm is used.

## 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.

## 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.

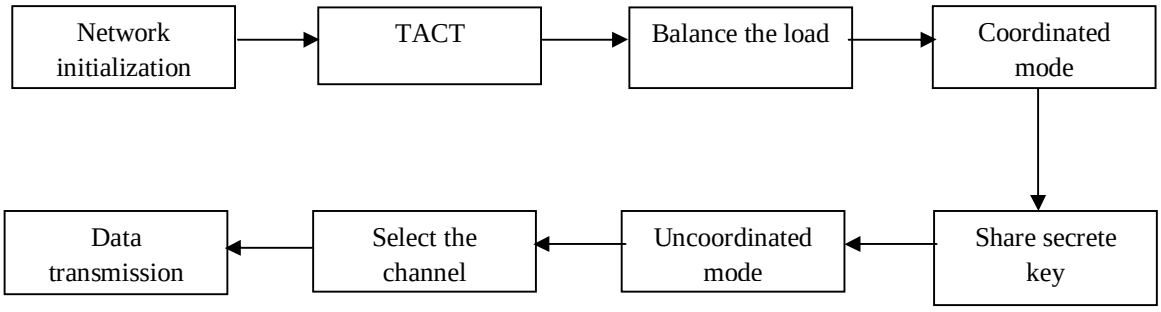


*Fig.1 System Architecture*

## 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 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.


 

**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 analyzed. Based on the analyzed 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

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.


 