International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 7 (2015) pp. 18231-18239
© Research India Publications
http://www.ripublication.com

Tackle The Deferral Messages Under Jamming Using TACT

Isaimathi. C[1], Narayanan. A. E[2], AP/IT, Anbaan. P[3]
[1] *Information technology, Periyar Maniammai University, Thanjavur , Tamilnadu 613403, India*
isai_0010@yahoo.co.in
[2] *Information technology, Periyar Maniammai University, Thanjavur, Tamilnadu 613403 , India*
aenan02@gmail.com
[3] *Server Administrator , Wipro Technologies , Sholinganallur, Chennai, Tamilnadu 600119 , India*
anban_me@yahoo.co.in

Abstract

Wireless networks introduce potential security vulnerabilities due to the shared nature of wireless channels. In wireless sensor network we have so many issues under jamming attacks. A wireless network that uses multiple frequency and code channels to provide jamming attacks resilience for smart grid applications (group of system connected in source provider). We have implement TACT method is used to overcome the message delay and network traffic. TACT is nothing but transmitting adaptive camouflage traffic .whenever the network bandwidth is below it is jammed at that time camouflage traffic is embedded with that network. The purpose of TACT is to verifying the delivery result of messages, avoid collusion and increase the traffic load. To finding the message delay we implement Timestamp in our project. To avoid the node coordination of jamming attacks using Gradient descent algorithm. It is popular and handles for very large-scale optimization problems. It is also known as steepest gradient mathematical method. Gradient descent algorithm in jamming attacks on encoding and decoding localization. It sequence of solutions that approach a traffic control without files or data destroyed. Using this algorithm, we can send and receive data, wherever we can select any source or destination at any time even other networks are transmitted data.

Keyword: Smart Grid, Transmitting adaptive camouflage traffic (TACT), message delay, Performance modeling, Gradient descent algorithm, Selective jamming attack.

Introduction

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. It involves the authorization of access to data in a network, which is controlled by the network administrator. wireless networks that provide flexible and unfettered network access have been proposed and designed for a variety of smart grid applications such as substation automation. However, the use of wireless networks introduces potential security vulnerabilities due to the shared nature of wireless channels. Indeed, 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. A smart grid is a modernized electrical grid that uses analogue or digital information and communications technology to gather and act on information, such as information about the behaviors of suppliers and consumers, in an automated fashion to improve the efficiency, reliability, economics, and Sustainability of the production and distribution of electricity. Smart grid is a vulnerable system and can be attacked even from aboard, attacks that may cause different level of issues and harms on the devices and society. So, research community has paid attention to this topic and the reasons of required security and privacy for the smart grid. Other security aspects like integrity, authorization and confidentiality can be implemented as long as a strong key management protocol has already been designed and addressed. A jammer is an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications A jammer continuously emits RF signals to fill a wireless channel so that legitimate traffic will be completely blocked Common characteristics for all jamming attacks is that their communications are not compliant with MAC protocols Jamming attacks can severely interfere with the normal operation of wireless networks and, consequently, mechanisms are needed that can cope with jamming attacks. 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. The characteristics of the virtual network topology and protocols together impede the attacker's ability to analyze traffic patterns, limit the visibility of real IP addresses to those cooperating hosts that are topologically adjacent to a host whose traffic is being monitored, and allow hosts to spread their IP identities and to modify the IPs associated with a host. These system characteristics will reduce the ability of a hostile entity to mount a successful denial-of-service attack against the operations among the set of hosts.

To solving a fundamental yet term for wireless smart grid applications: how to minimize the message delay under worst-case jamming attacks. We have implement TACT method is used to overcome the message delay and network traffic. TACT is nothing but transmitting adaptive camouflage traffic whenever the network bandwidth

is below it is jammed at that time camouflage traffic is embedded with that network. The purpose of TACT is to verifying the delivery result of messages, avoid collusion and increase the traffic load. To avoid the node coordination of jamming attacks using Gradient descent algorithm Using this algorithm, we can send and receive data, wherever we can select any source or destination at any time even other networks are transmitted data. and also it deployed gradient descent methodology using this we can classify the traffic in network. routine traffic for network monitoring and control.

Probing traffic for performance measurement, its message transmission time equals to time limit. Before sending the packets the source should know the all node status whether the node is normal or busy that can be called as Routine Traffic. In source node the file is transfer with Time limit in encoding format and while decoding the file it is analyzed by probing the traffic. To overall network traffic is balanced by camouflage traffic.

Existing System

There have been extensive works on designing spread spectrum based communication schemes, which provide jamming resilience to conventional wireless networks by using multiple orthogonal frequency or code, channels. In other words, based on commonly-adopted jamming attack models (e.g., periodic, memory less, and reactive models), existing works focus on designing anti jamming communication schemes for message delivery in conventional wireless networks.

Proposed System

In this paper, we address this issue by considering a wireless network that uses multiple frequency and code channels to provide jamming resilience for smart grid applications. We implement TACT is to verifying the delivery result of messages, avoid collusion and increase the traffic load. and To finding the message delay we implement Timestamp in this paper. To avoid the node coordination of jamming attacks using Gradient descent algorithm. Using this algorithm, we can send and receive data, wherever we can select any source or destination at any time even other networks are transmitted data.

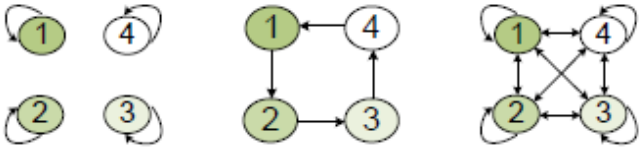
Gradient Descent Algorithm

Gradient descent algorithm is popular and handles for very large-scale optimization problems. It is also known as steepest gradient mathematical method. Gradient descent algorithm in jamming attacks on encoding and decoding localization. It sequence of solutions that approach a traffic control without files or data destroyed. The basic idea of Gradient Descent is to use a loop to adjust the model based on he error it observes between its predicted output and the actual output. The adjustment node is pointing to a direction where the error is decreasing in the steepest sense (hence the term "gradient").

It defined so this approach can be applicable in a wide range of machine learning scenarios.

- The Model
- The loss function
- The learning rate

Gradient Descent is very popular method because of the following reasons Intuitive and easy to understand. Easy to run incrementally with additional data On the other hand, the greedy approach in Gradient Descent can be trapped in local optimum. This can be mitigated by choosing a convex LOSS function (which has a single node), or multiple starting points can be picked randomly generated.

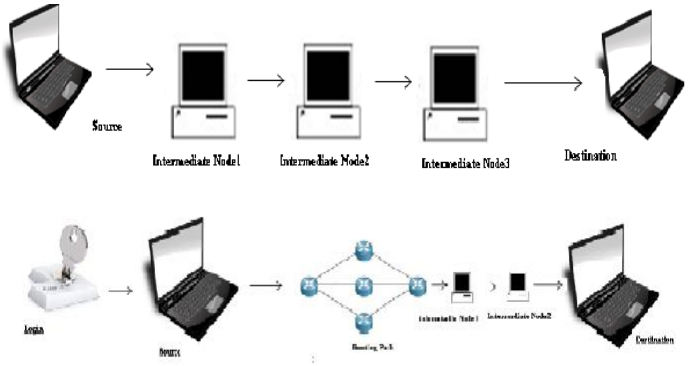


(a).Constant/Wireless Jamming (b).Wired/Sweeping Jamming (c) Uniformly Distributed Jamming

Workflow Descriptions

Routing Path

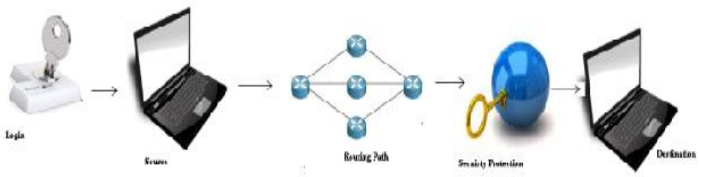
Consider a network, where is a set of nodes and is a set of directed links connecting the nodes. A sensor networks, are characterized by continuous data streaming from multiple sources and through intermediate processing by multiple aggregators. It is widely used for enabling multiple users to transmit packet simultaneously on the same frequency range by utilizing distinct sequences.



Security Protection

The network interference is a primary security threat to prevent the deployment of wireless networks in the smart grid. This primary security is one of the security protections. When this data is sending information source to destination it will be configured to start automatically. Such a static encoding of data leads to a highly

regular behavior in the message delays, whereas overt traffic arrives anytime, resulting in an irregular pattern.

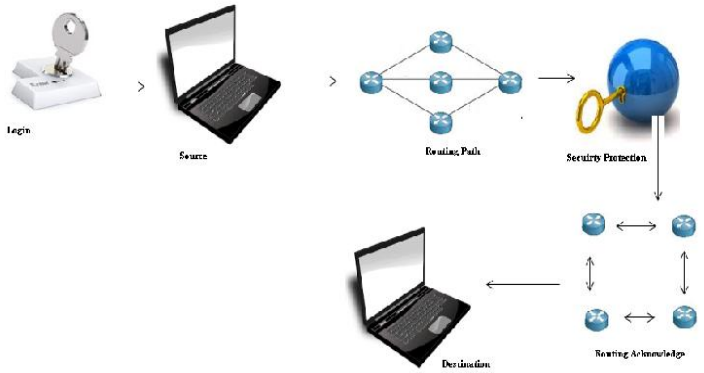


Message Delay

The context of sensor networks as information about the source node and the nodes that processed/forwarded the data throughout its transmission. 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.

Routing Acknowledgment

In wireless communication environment, all the nodes within the communication range of the transmitter have the same probability to be the real packet receiver. Routing Acknowledgement is used to find the node is received the data or not .if the node received the data it will change the mode, if it is not received it will remain the same mode.



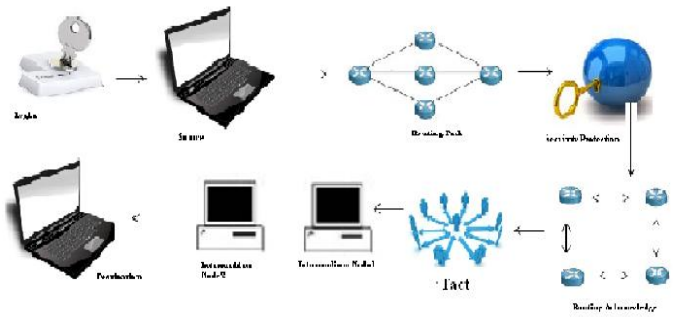
TACT Classification

Wireless monitoring for substation transformers only needs to transmit a message every second. This indicates that in general, we should intentionally increase a certain amount of redundant traffic to obtain the optimal traffic load.

A legitimate message can have a chance to be successfully delivered during the period that jamming attacks attempt to disrupt redundant traffic. We name such traffic as *camouflage traffic* since it serves as camouflage to "hide" legitimate traffic from

attacks. While transmitting, a node may send the sensed data or pass an aggregated data value computed from routing node.

The packet is also time stamped by the source node with the generation time. The sequence of gradient descent is the communication channel is the signal transmitted through it classification



System Analysis

Feasibility Study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- Economical Feasibility
- Technical Feasibility
- Social Feasibility

Economical Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The

developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

System Architecture

Source and destination is used to transfer the data using routing path Routing path is used to select the path to reach the destination. Security protection is used to whenever we choose the file it will generate a key for each file. so the file will be secured. TACT is used to overcome the issues of traffic congestion, message delay so we used timestamp and error correction.

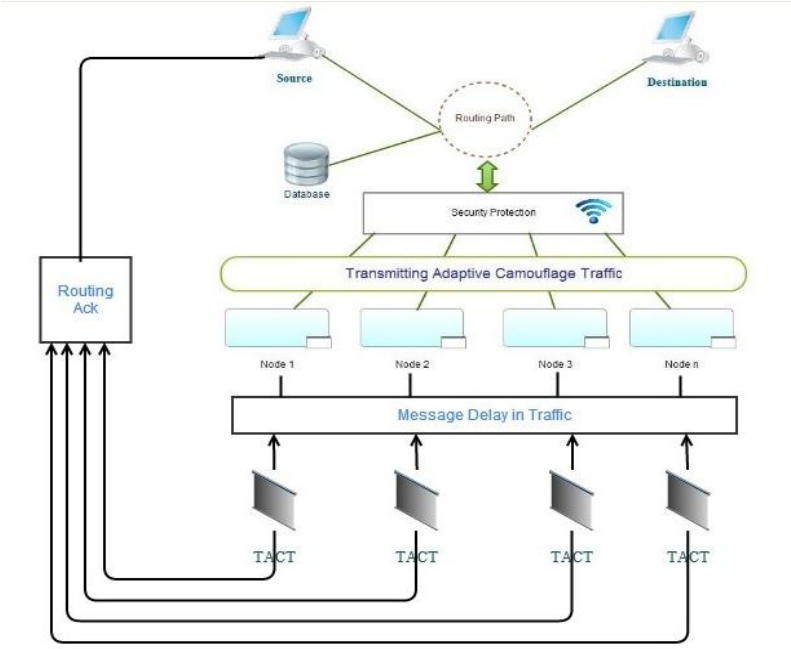


Figure 7.1: Transmitting adaptive camouflage traffic (TACT)

Discussions

Our goal is not to design a commercial anti-islanding system, but to demonstrate a proof-of-concept application of TACT in the smart grid. We observed that TACT achieved nearly-optimal performance. It is challenging to design an adaptive method

that always works at the optimal load. However, the concept of transmitting camouflage traffic can lead to more TACT-like methods to further improve the delay performance for wireless smart grid applications.

Camouflage traffic is blind to all legitimate receivers and attackers, which is the simplest setup for the attackers to have no ability to identity legitimate traffic from Camouflage traffic, which on the other hand causes collisions between legitimate and camouflage traffic transmissions. We will explore smart ways to avoid such collisions in the future work.

We also emphasize that our methodology in this paper is to optimize the Gradient-Descent Algorithm to offer performance guarantee for smart grid applications. Therefore, our Gradient-Descent Algorithm does not necessarily means a uniformly optimal solution to all cases. This indicates that when a jammer constantly changes its jamming behavior, our countermeasure may not keep providing optimal solutions against each behavior. we design our counter measures based on the Algorithm, we can always provide performance guarantee under any attack behavior, which is our goal and also essential for smart grid applications.

Future Enhancement:

Future work may incorporate Schemes like genetic approach to trace back on an all topology. Efficient packet marking technique by occasionally TACT with special edge id representing a link between the router and the input port on which the packet has arrived. Pre shared key authentication mechanism in mobile the selective jamming/dropping attacks can be launched by performing real-time packet classification at the layer. Real-time packet classification can be mapped to the hiding property of commitment methods and propose a packet-hiding method based on commitments.

Conclusion

We conclude TACT method is used to overcome the message delay and network traffic. TACT is nothing but transmitting adaptive camouflage traffic .whenever the network bandwidth is below it is jammed at that time camouflage traffic is embedded with that network. The purpose of TACT is to verifying the delivery result of messages, avoid collusion and increase the traffic load.

References

[1] X. Lu, W. Wang, and J. Ma, “Authentication and integrity in the smart grid: An empirical study in substation automation systems,” International J. Distributed Sensor Networks, Apr.2012

[2] W. Wang, Y. Xu, and M. Khanna, “A survey on the communication architectures in smart grid,” Computer Networks, 2011.

[3] NIST Smart Grid Cyber Security Working Group, "Guidelines for smart grid cyber security," NIST IR-7628, vol. 1-3, Aug. 2010.

[4] B. Akyol, H. Kirkham, S. Clements, and M. Hadley, "A survey of wireless communications for the electric power system," in Tech.Report, Pacific Northwest National Laboratory, Jan. 2010.

[5] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication protocols and networks for power systems - current status and future trends," in Proc. of Power Systems Conference & Exposition, 2009.

[6] J.T.Chiang and Y.-C.Hu,"Dynamic jamming mitigation for wireless broadcast networks," in Proc. of IEEE INFOCOM, 2008

[7] R.Priyadarshini, A.Prabhagaran, A.Lavanya, Boopathi for Minimization of Jamming Attack in Wireless Broadcast Networks Using Neighboring Node Technique in IEEE May 2012

[8] Jokar, P, Beznosov, K, Leung, V.C.M, for Efficient Authentication and Key Management Mechanisms for Smart Grid Communications in IEEE July 2013.

[9] Yalin Evren Sagduyu , Randall A. Berry and Anthony Ephremides for "Wireless Jamming Attacks under Dynamic Traffic Uncertainty" in IEEE Dec 2008.

[10] Justin Raj S.S., D. Thilagavathy for "Security Threats and Jamming attacks Of Multi Channel Wireless Sensor Networks" in IEEE May 2012.

[11] Nicanfar, H. , Vancouver, Jokar, P. ; Beznosov, K. ; Leung, V.C.M. for **"**Efficient Authentication and Key Management Mechanisms for Smart Grid Communications" in IEEE July 2013.

[12] Kim Pecina,Esfandiar Mohammadi,Christina Pöpper for "Zero-Communication Seed Establishment for Anti- Jamming Techniques" in IEEE conference, May 2013.

[13] Zhuo Lu, Xiang Lu ,Wenye Wang , Wang, C., for " Review and evaluation of security threats on the communication networks in the smart grid" in IEEE conference,Oct-Nov 2010.

[14] Nadeem Sufyan , Nazar Abbass Saqib and Muhammad Zia for "Detection of jamming attacks in 802.11b wireless networks" *EURASIP Journal on Wireless Communications and Networking* 2013, 2013.

[15] Domenico Giustiniano ETH, Thun, B.Schmitt TU, Michael Suhler ETH, and Matthias Wilhelm TU for "Detection of reactive jamming in DSSS-based wireless networks" in Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, WiSec'13.

[16] Loukas Lazos, Sisi Liu, and Marwan Krunz for "Mitigating Control-Channel Jamming Attacks in Multi-channel Ad Hoc Networks"in WiSec'09, March 16–18, 2009.