International Journal of Current Trends in Engineering & Research (IJCTER)
e-ISSN 2455–1392 Volume 2 Issue 3, March 2016 pp. 6 - 11
Scientific Journal Impact Factor : 3.468
http://www.ijcter.com

MININIZING THE MESSAGE DELAY BY USING SMARD GRID APPLICATION

R.SASIKALA[1], C.SASIKUMAR[2], M. DHARINIPRIYA[3], S.P. SANTHOSHKUMAR[4]

[1]*UG Scholar, Dept of CSE, Shree Sathyam College of Engineering and Technology, Sankari, India.*
[2,3]*Assistant Professor, Dept of CSE, Shree Sathyam College of Engineering and Technology, Sankari, India*
[4]*HOD, Dept of CSE, Shree Sathyam College of Engineering and Technology, Sankari, India*

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)**. A synergistic combination of multipath relay transmissions, K-out-of N message encoding, packet encryption, heteromorphy packet relay and dynamically assignable IP addresses. 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. By defining a generic overcrowding process that characterizes a wide range of existing jamming models, we show that the worst-case message delay is a U-shaped function of network traffic load. This indicates that, interestingly, increasing a fair amount of redundant traffic, called camouflage, can improve the worst-case delay performance.

Keywords: Smart Grid, potential security, wireless networks, spread spectrum, overcrowding process, jamming models

I. INTRODUCTION

The smart grid is an up-and-coming cyber physical system that integrates power infrastructures with in order technologies. In the smart grid, wireless networks have been proposed for efficient communications. However, the congestion attack that broadcasts radio interference is a primary security threat to prevent the deployment of wireless networks. Hence, spread spectrum systems with overcrowding resilience must be adapted to the smart grid to secure wireless communications. There have been extensive works on designing spread spectrum schemes to achieve feasible communication under jamming attacks. Nevertheless, an open question in the smart grid is how to minimize message delay for timely communication in power applications. In this paper, we address this problem in a wireless network with spread spectrum systems for the smart grid. By defining a generic overcrowding process that characterizes a wide range of existing jamming models, we show that the worst-case message delay is a U-shaped function of network traffic load[2],[3]. This indicates that, interestingly, increasing a fair amount of redundant traffic, called camouflage, can improve the worst-case delay performance. We demonstrate via experiments that transmitting camouflage traffic can decrease the probability that a message is not delivered on time in order of magnitude for smart grid applications[4].

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[4].

The disadvantage of the existing system the existing traffic classification methods suffer from poor performance in the crucial situation where supervised information is insufficient and considerable unknown flows are present. Transport protocol ports for classification purposes became unreliable while different kinds of new network applications were emerging. The advantage of the existing system. The enforcement of security policies on the use of different applications, The ability to classify encrypted traffic and the identification of malicious traffic flows.

II. LITERATURE SUVERY

2.1 On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage

Using cloud storage, data owners can remotely store their data and enjoy the on-demand high quality cloud services without the burden of local data storage and maintenance. However, this new paradigm does trigger many security concerns. A major concern is how to ensure the integrity of the outsourced data. To address this issue, recently, a highly efficient dynamic auditing protocol (IEEE Transactions on Parallel and Distributed Systems, doi:10.1109/TPDS.2013.199) for cloud storage was proposed which enjoys many desirable features[1]. Unfortunately, in this letter, we demonstrate that the protocol is insecure when an active adversary is involved in the cloud environment. We show that the adversary is able to arbitrarily modify the cloud data without being detected by the auditor in the auditing process. We also suggest a solution to fix the problem while preserving all the properties of the original protocol.

2.2 Performance and Cost Evaluation of an Adaptive Encryption Architecture for Cloud Databases

The cloud database as a service is a novel paradigm that can support several Internet-based applications, but its adoption requires the solution of information confidentiality problems. We propose a novel architecture for adaptive encryption of public cloud databases that offers an interesting alternative to the tradeoff between the required data confidentiality level and the flexibility of the cloud database structures at design time[2],[3]. We demonstrate the feasibility and performance of the proposed solution through a software prototype. Moreover, we propose an original cost model that is oriented to the evaluation of cloud database services in plain and encrypted instances and that takes into account the variability of cloud prices and tenant workloads during a medium-term period.

2.3 Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases

Placing critical data in the hands of a cloud provider should come with the guarantee of security and availability for data at rest, in motion, and in use. Several alternatives exist for storage services, while data confidentiality solutions for the database as a service paradigm are still immature. We propose a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data[3],[4]. This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute concurrent and independent operations including those modifying the database structure. The proposed architecture has the further advantage of eliminating intermediate proxies that limit the elasticity, availability, and scalability properties that are intrinsic in cloud-based solutions.

2.4 An Efficient Certificate less Encryption for Secure Data Sharing in Public Clouds

We propose a mediated certificate less encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Mediated certificateless public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations or vulnerable against partial decryption

attacks. In order to address the performance and security issues, in this paper, we first propose a mCL-PKE scheme without using pairing operations. We apply our mCL-PKE scheme to construct a practical solution to the problem of sharing sensitive information in public clouds. The cloud is employed as a secure storage as well as a key generation center[6].

2.5 Privacy-Preserving Multi-Class Support Vector Machine for Outsourcing the Data Classification in Cloud

Emerging cloud computing infrastructure replaces traditional outsourcing techniques and provides flexible services to clients at different locations via Internet. This leads to the requirement for data classification to be performed by potentially untrusted servers in the cloud[7]. Within this context, classifier built by the server can be utilized by clients in order to classify their own data samples over the cloud. In this paper, we study a privacy-preserving (PP) data classification technique where the server is unable to learn any knowledge about clients' input data samples while the server side classifier is also kept secret from the clients during the classification process. More specifically, to the best of our knowledge, we propose the first known client-server data classification protocol using support vector machine

III. MODELS AND PROBLEM FORMULATION

3.1 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.

3.2 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.

3.3 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

3.4 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[11]. 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.

Algorithm: TACT at Each Node

Given: Camouflage traffic load L, L_{min} and L_{max}
Given: Traffic increment $_{inc}$ and decrement $_{dec}$
Initialization: Mprev, L Lmin
repeat
Transmit probing message in an observation period
Measure the number of ACKs, M_{now},
if performance not degraded (M_{now} >/M_{prev}) **then**
Increase the traffic load: L min(L+inc, Lmax)
else
Decrease the traffic load: L max(L-dec,min)
endif
Record history Mprev Mnow
until TACT is diabled

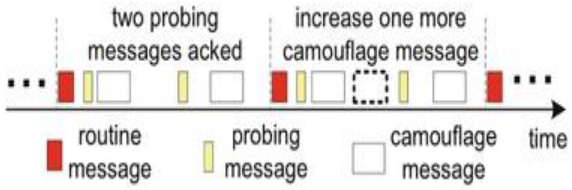

Figure1: Diagram To Illustrate How TACT balance the network traffic

3.5 System design

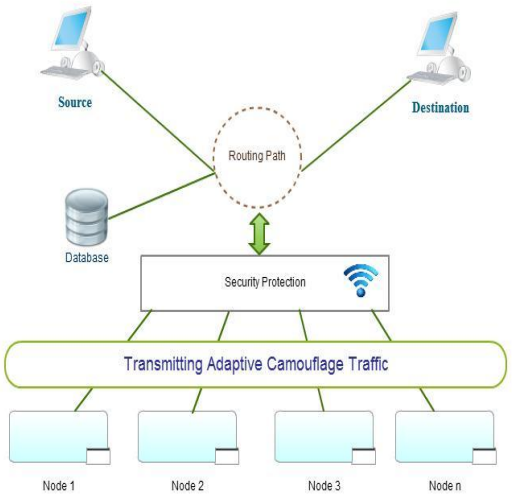

Figure 2: Transmitting adaptive camouflage traffic system

IV. 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 [8],[10]. 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 the 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.

Gradient descent is based on the observation that if the multi-variable function $F(\mathbf{x})$ is defined and differentiable in a neighborhood of a point $\mathbf{a}$, then $F(\mathbf{x})$ decreases *fastest* if one goes from $\mathbf{a}$ in the direction of the negative gradient of F at $\mathbf{a}$, $-\nabla F(\mathbf{a})$. It follows that, if

$$\mathbf{b} = \mathbf{a} - \gamma \nabla F(\mathbf{a}) \qquad (1)$$

For γ small enough, then $F(\mathbf{a}) \geq F(\mathbf{b})$. In other words, the term $\gamma \nabla F(\mathbf{a})$ is subtracted from $\mathbf{a}$ because we want to move against the gradient, namely down toward the minimum. With this observation in mind, one starts with a guess $\mathbf{x}_0$ for a local minimum of F, and considers the sequence $\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \cdots$ such that

$$\mathbf{x}_{n+1} = \mathbf{x}_n - \gamma_n \nabla F(\mathbf{x}_n), \ n \geq 0. \qquad (2)$$

We have

$$F(\mathbf{x}_0) \geq F(\mathbf{x}_1) \geq F(\mathbf{x}_2) \geq \cdots, \qquad (3)$$

So hopefully the sequence $(\mathbf{x}_n)$ converges to the desired local minimum. Note that the value of the *step size* γ is allowed to change at every iteration. With certain assumptions on the function F (for example, F convex and ∇F Lipschitz) and particular choices of γ (e.g., chosen via a line search that satisfies the Wolfe conditions), convergence to a local minimum can be guaranteed. When the function F is convex, all local minima are also global minima, so in this case gradient descent can converge to the global solution.

This process is illustrated in the picture to the right. Here F is assumed to be defined on the plane, and that its graph has abowl shape. The blue curves are the contour lines, that is, the regions on which the value of F is constant. A red arrow originating at a point shows the direction of the negative gradient at that point. Note that the (negative) gradient at a point is orthogonal to the contour line going through that point[9]. We see that gradient *descent* leads us to the bottom of the bowl, that is, to the point where the value of the function F is minimal.

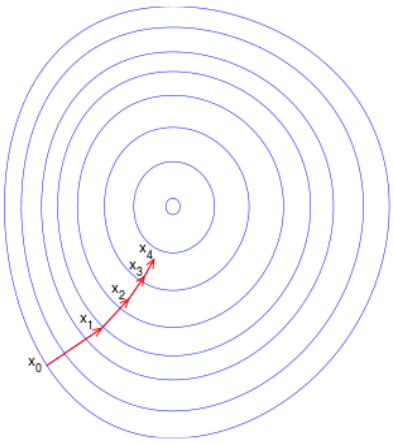

Figure 3: Illustration of gradient descent

V. CONCLUSION

In this paper, we provided 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.

REFERENCES

[1] Zhuo Lu Wenye Wang,Cliff Wang, "Hiding Traffic with Camouflage: Minimizing Message Delay in the Smart Grid under Jamming", The 31st Annual IEEE International Conference on Computer Communications: Mini-Conference.978-1-4673-0775-8/12/$31.00 ©2012 IEEE.

[2] 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 and Exposition, Mar. 2009.

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

[4] P. M. Kanabar, M. G. Kanabar, W. El-Khattam, T. S. Sidhu, and A. Shami, "Evaluation of communication technologies for IEC 61850 based distribution automation system with distributed energy resources," in Proc. of IEEE PES General Meeting, 2009.

[5] NIST News Release, "Smart grid panel agrees on standards and guide-lines for wireless communication, meter upgrades," Apr. 19 2011.

[6] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. of ACM MobiHoc '05, 2005, pp. 46–57.

[7] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in Proc. of IEEE INFOCOM '10, Mar. 2010.

[8] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in Proc. of IEEE Symposium on Security and Privacy, May 2008, pp. 64–78. IEC Standard, "IEC 61850: Communication networks and systems in substations," 2003.

[9] T. S. Sidhu and Y. Yin, "Modelling and simulation for performance evaluation of IEC61850-based substation communication systems," IEEE Trans. Power Delivery, vol. 22, no. 3, pp. 1482–1489, July 2007.

[10] F. Cleveland, "Enhancing the reliability and security of the information infrastructure used to manage the power system," in Proc. of IEEE PES General Meeting, June 2007.

[11] "Uses of wireless communications to enhance power system reliability," in Proc. of IEEE PES General Meeting, June 2007.