IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 3, June 2019
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

An Approach Minimizing Message Delay for Smart Grid Applications under Jamming

[1] Nidhi Khera; [2] Hemlata Dakhore

[1] G.H. Raisoni Institute of Engineering and Technology,
Nagpur, Maharashtra, India

[2] G.H. Raisoni Institute of Engineering and Technology,
Nagpur, Maharashtra, India

Abstract - The smart grid is a giant "System of systems" which enables bidirectional communication methods and control capabilities with innovative deployment of cyber systems and power infrastructures with the wireless communication technologies. The constant interfering nature of jammers in the radio frequency in wireless networks creates jamming havoc in the smart grid communication system. Hence the spread spectrum techniques that uses orthogonal multiple frequency and pseudo code channels must be used in the smart grid communication systems to provide secure communication with required timing constraints for control messages. The critical problem is to minimize the message delay for timely smart grid applications under the influence of vulnerable jamming attacks. For solving this issue, we provide a reliable technique of transmitting adaptive camouflage traffic (TACT) which provides delay performance guarantee for timely smart grid applications under any kind of worst case jamming attack. We first define a generic jamming process then study the worst case methodology of jamming attacks using TACT which shows that the worst case message delay is a U-shaped function of the network traffic load at the optimum. Further the collisions between the legitimate and camouflage traffic can be avoided using message concatenation which again reduces the delay performance in the smart grid communication.

Keywords - *Smart grid, wireless networks, generic jamming, worst case methodology, message concatenation.*

1. Introduction

The smart grid is a large 'System of Systems' that enables bidirectional flows of energy and uses a bidirectional communication method and control capabilities that leads to an array of new functionalities and numerous applications The smart grid is an innovative cyber-physical system that incorporates networked control mechanisms (e.g. advanced metering and demand response) into conventional power infrastructures [1]. To facilitate information delivery for such mechanisms, wireless networks that provide flexible and untethered network access have been proposed and designed for a variety of smart grid applications[1], [7], such as substation automation [1], [7] and home metering [2]. As a result, wireless networks have become an essential integration to the communication infrastructure for the smart grid.

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 [1], [6] that the jamming attack, which uses radio interference to disrupt wireless communications [2], [3], 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. How to defend against jamming attacks is of critical importance to secure wireless communications in the smart grid. 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 [2], [1] or code [3], [4] channels. Interesting enough, most efforts adopt a case-by case (or model-by-model) methodology to investigate how a message can be sent to its destination. 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.

But, 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 (as much as possible) [1]. 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.

Under the threat of attacker efforts to jam mission- or safety critical wireless transmissions (such as emergency alerts or navigation signals), Spread Spectrum (SS) techniques represent a common way to achieve anti-jamming communication [1]–[4]. Anti-jamming communication is used in commercial and military applications, both between paired devices and from one sender to multiple receiving devices (in multicast or broadcast settings). Spread spectrum techniques use data-independent, random sequences to spread a narrowband information signal over a wide (radio) band of frequencies. Under the premise that it is hard or infeasible for an attacker to jam the entire frequency band, the receiver can correlate the received signal with a replicate of the random sequence to retrieve the original information signal. Important instances of spread spectrum techniques are Frequency Hopping (FH) and Direct-Sequence Spread Spectrum (DSSS). Essential for both FH- and DSSS-based communication is that the sender and the receiver share a secret prior to their communication which enables the receiver to generate the random sequence and to detect and decode the sender's spread signal. This reliance on a pre-shared secret generally precludes unanticipated transmissions between unpaired devices as well as communication from a sender (or base station) to an unknown set of receivers (some of which might be malicious and try to compromise the receptions of other receivers).

This problem can best be illustrated as follows: If a base station wants to broadcast a message to a set of receivers in a jamming-resistant manner, it would need to share one or several secret spreading sequences with all the receivers, and the sequences would need to be hidden from the attacker (that could otherwise jam the transmissions using the spreading sequences). In a number of scenarios—such as in those where receivers cannot be trusted or where they are unknown before the actual communication (e.g., in local or global navigation systems) the assumption about shared secret spreading sequences is unrealistic and typically prevents the application of anti-jamming communications. Wireless communications is vulnerable to jamming attacks due to the shared use of wireless medium. A jammer can simply take advantage of a radio frequency (RF) device (e.g. a waveform generator) to transmit signals in the wireless channel. As a result, signals of the jammer and the sender collide at the receiver and the signal reception process is disrupted. Therefore, jamming resistance is crucial for applications where reliable wireless communications is required. Spread spectrum techniques have been used as countermeasures against jamming attacks.

Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) are two examples of spread spectrum techniques. In classic spread spectrum techniques, senders and receivers need to pre-share a secret key, with which they can generate identical hopping patterns, spreading codes, or timing of pulses for communication. However, if a jammer knows the secret key, the jammer can easily jam the communication by following the hopping patterns, spreading codes, or timing of pulses used by the sender. There have been a few recent attempts to remove the dependency of jamming-resistant communications on pre-shared keys [4], Thus an Uncoordinated Frequency Hopping (UFH) technique has been developed to allow two nodes that do not have any common secret to establish a secret key for future FHSS communication in presence of a jammer independently use similar coding techniques to improve the robustness and efficiency in UFH [4]. This successfully removes the requirement of pre-shared keys in point-to-point FHSS communication. Unfortunately, UFH and its variations cannot be directly used for broadcast communication, since their primary objective is to establish a pairwise key between two parties. Indeed, any spread spectrum communication system that requires a shared key, either pre-shared or established at the initial stage of the communication, cannot be used for broadcast communication where there may be insider jammers. Any malicious receiver, who knows the shared key, may use the key to jam the communication. To address this problem, researchers recently investigated how to enable jamming-resistant broadcast communication without shared keys [1], [4].

However, the decoding process of the method is inherently sequential (i.e., the decoding of the next bit depends on the decoded values of the previous bits). Though it works with short pulses in the time domain, the method cannot be extended to DSSS or FHSS without significantly increasing the decoding cost. Hence an Uncoordinated Direct Sequence Spread Spectrum (UDSSS) approach, that avoids jamming by selecting a spreading code sequence from a pool of code sequences in a randomized manner. But, UDSSS is more prone to reactive jamming attacks, it is observed that when the jammer does not have sufficient

computational power to infer the spreading sequence quickly enough, UDSSS still provides good enough jamming resistance. However, when the jammer has sufficient computational power, UDSSS fails to provide strong guarantee of jamming resistance.

Many operators, homeowners, workforce field engineers, service providers and marketing staff require access to the operating software packages and tools via many access points. Such access imposes serious cyber security threats that require authentication and authorization to protect the grid from any cyber-attacks [5].

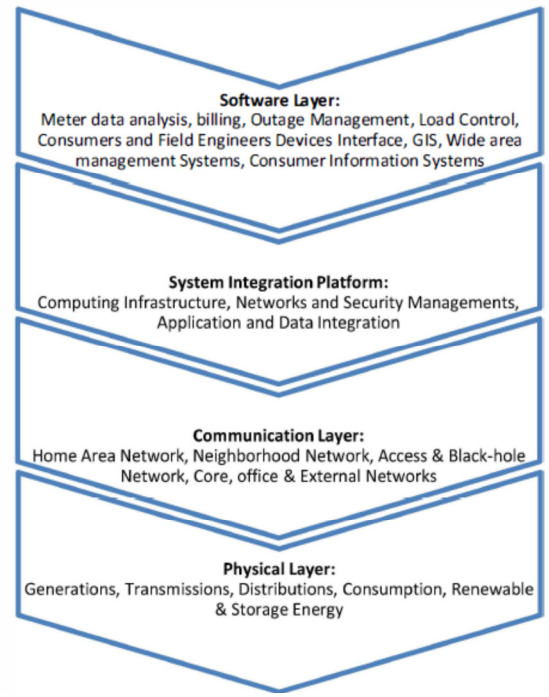

Figure 1:- A Smart grid conceptual model

In this paper, our focus is to solve the fundamental and an open question for wireless smart grid applications: how to minimize the message delay under worst case jamming attacks, [1], [7]. The solution on this question cannot only help us design network strategies against worst-case jamming attacks in wireless smart grid applications, but also We channelize this issue by considering a wireless network that uses orthogonal multiple frequency and code channels to provide jamming resilience for smart grid applications. We consider two general jamming-resilient communication modes it is 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.

As power applications are restricted with time-critical with strict timing requirements (e.g., 3 and 10 ms in substation automation protection), message delivery becomes invalid as long as its delay D is greater than the delay threshold s. Therefore, different from existing metrics (e.g., throughput or packet delivery ratio [7]) to evaluate the jamming impact in conventional wireless networks, we use the message invalidation probability PðD > sÞ, which directly reflects timing requirements of power applications, to measure the jamming impact in the smart grid. Our goal is to minimize PðD > sÞ under the worst-case jamming attack. To this end, we first define a generic jamming process that includes a wide range of existing jamming models. Then, we provide an experimental study to show PðD > sÞ and accordingly design a solution to minimize PðD > sÞ under jamming attacks. We highlight our major study as follows:

1) We propose to study the worst-case performance under a generic jamming process. We show that the worst-case performance in terms of message invalidation probability exhibits a U-shaped response to aggregated network traffic load. In order words, the message invalidation probability is first decreasing, then-increasing function of network traffic load for smart grid applications: coordinated and uncoordinated modes [2], [3], [4], [7]. In coordinated mode, the sender and receiver share a common secret or key (e.g. code-frequency channel assignment), which is unknown to attackers. Accordingly, an attacker has to choose its own strategy to disrupt the communication between the transmitter and receiver. Coordinated communication is a conventional model in spread spectrum systems. However, the transmitter and receiver may not share a common secret initially.

2)Based on this U-shape effect, we propose a transmitting adaptive camouflage traffic (TACT) system that uses “camouflage traffic” to achieve the optimal aggregated network traffic load to minimize the message invalidation ratio.

The underlying explanation behind the U-shape phenomenon and the TACT anti-jamming strategy is that using camouflage traffic (i.e., redundant traffic transmitted by TACT) is the over-provision of bandwidth in a smart grid network, where time-critical traffic rate is smaller than the network bandwidth. By sending more such camouflage traffic (mixed with smart grid control traffic) to the network, we can force a jammer to“waste” enough jamming capability on the camouflage traffic (because the

jammer has no way to tell the camouflage traffic from the real smart grid traffic), so that the jammer cannot find the real traffic quickly enough. Therefore, the message invalidation ratio decreases when we send camouflage traffic into the network under jamming. However, if the rate of sending the camouflage traffic keeps increasing and approaches the network bandwidth, more network collisions will happen in the network, thereby degrading the network performance (i.e., increasing the message invalidation ratio). As a result, there exists an optimal rate to send camouflage traffic and TACT is used to adaptively find this rate. Because our strategy is based on the worst-case methodology, the U-shape property and the global minimum of the message invalidation probability are independent with a particular jamming strategy, thus offering performance guarantee for a wireless smart grid application under jamming attacks.

2. Models and Problem Definition

In this section, we first introduce backgrounds on wireless networks for the smart grid, then present the network and jamming models, finally formulate the problem.

2.1 Backgrounds: Wireless network for Smart Grid

Wireless networks are in general used for local-area smart grid applications, such as substation automation and distributed energy management [1], [7]. The wireless network for a local-area power system consists of a number of intelligent electronic devices (IEDs) and the gateway node. IEDs are devices installed on infrastructures to fulfill power management procedures by communicating with each other. The gateway is connected to the smart grid backbone network.

Local-area messages can be forwarded via the gateway to outside networks. Due to the broadcast nature of wireless channels, wireless networks for the smart grid are inevitably exposed to jamming attacks, which transmit radio interference to prevent legitimate messages from being received [2], [3], [7]. It has already been pointed out that jamming attacks, by interfering communication between power equipment, can possibly result in grid operation instability or even regional blackout. Therefore, wireless networks for the smart grid must have the ability to combat jamming attacks. There are two widely-used spread spectrum techniques [2], [3], to defend against jamming attacks in the literature. (i) Frequency hopping spread spectrum (FHSS): the sender and receiver switch a frequency channel among a pool of candidate channels from time to time. The jammer can only jam a transmission when it is on the same channel. (ii) Direct sequence spread spectrum (DSSS): the sender multiplies the original data with a pseudo-noise (PN) sequence (called a code channel). The receiver uses a co-relator with the same PN sequence to recover the original message. It is difficult for a jammer to disrupt the communication unless it knows the PN sequence used by the channel. Both FHSS and DSSS have been proposed and used for power applications [3]. For example, a DSSS based system is demonstrated in [17] for local substation automation. Since FHSS and DSSS provide jamming resilience by using multiple orthogonal frequency and code channels, a trivial solution for decreasing the message delay is to increase the number of frequency or code channels. Then, a jammer will have a lower chance to transmit jamming signals on the same channel used by transmit-receive pair. However, it is quite undesirable in practice because of the large cost of network spectrum resources. Therefore, we attempt to minimize the message delay in a wireless network with fixed numbers of frequency and code channels.

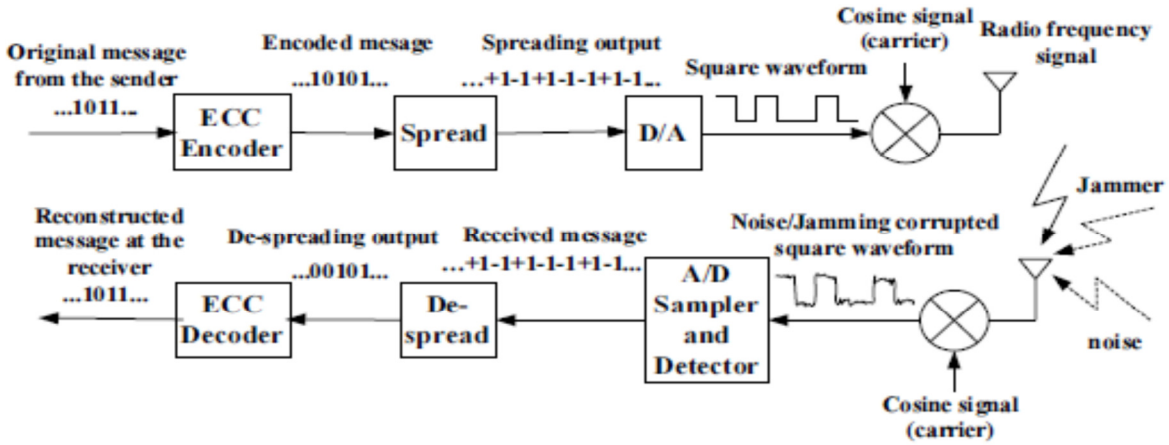

Figure 2:- Simple communication framework of DSSS

2.2 Network Model

We consider a wireless local-area network Nðm;Nf; NcÞ, where m is the number of nodes (including IEDs and the gateway) in the network, Nf and Nc are the numbers of frequency and code channels, respectively. There are two major types of traffic flows in the network: 1) Local traffic, which is generated from one node to another for local monitoring or protection; 2) Outside traffic, which is between a node and an outside node via the smart grid backbone network.

For a message going outside, it will be delivered first from an IED to the gateway via the local-area network (local delivery), then to the destination network via the smart grid backbone network. If there exists a jammer, it can affect the delay performance of both local and outside traffic types. For outside traffic, the delay component for the first local delivery can dominate in the overall end-to-end delay, since the smart grid backbone network is always of high bandwidth. Therefore, we focus on the message delay of local traffic in the network. It is worth noting that in the smart grid, a large amount of network traffic features a constant traffic model for continuous monitoring and control of power equipment [1], [7].

In addition, nodes can have distinct network traffic loads for different applications. For example, merging unit IEDs in a substation can send data of sampled power signal quality at various rates of 960-4,800 messages\s, dependent on configuration [9]. Thus, we assume that there are heterogeneous traffic loads in network Nðm;Nf;NcÞ; i.e., node i has a constant traffic load of _i messages/s (i 2 f1; 2; . . .;mg) in the network.

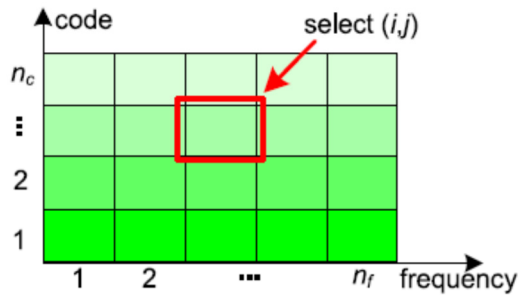

Figure 3:-Available frequency Nf and code Nc channels

2.3 Generic Jamming Model

The objective of a jammer is to broadcast interference to disrupt messages as many as possible in network Nðm;Nf;NcÞ. As the network has multiple channels, the jammer can adopt a wide range of strategies. In the literature, there are two major jamming types in terms of jamming behavior: non-reactive and reactive models [1] [2], [3], [7]. Non-reactive jammers transmit radio interference by following their own strategies. Reactive jammers transmit interference only when they sense any activity on a wireless channel. In addition, a jammer can either target a single frequency-code channel or have the ability to attack multiple channels at the same time. In this paper, we assume that the jammer has the knowledge of the pool of candidate channels used in the network, and attempt to choose the best strategy to attack one or some of the channels and lead the worst-case attack. In order to adopt varying strategies the jammer can use, we define a generic process to accommodate various jamming behaviors and models in the literature.

2.4 Problem Description

The primary goal of smart grid communication is to achieve timely monitoring and control for power control applications. Therefore, the delay performance is of critical importance in the smart grid. A time-critical message becomes invalid as long as its message delay D is greater than its delay constraint s. As a result, we focus on how to minimize the message invalidation probability PðD> sÞ in network Nðm;Nf;NcÞ under the generic jamming process ððF; CÞ;XÞ. It is noteworthy that the network operator always attempts to minimize the message delay; in contrast, the jammer always intends to maximize the message delay. The lowest bound of the message delay is always achieved when there is no jammer or a native jammer. As the NIST requires smart grid operations must continue under any potential attack, we adopt a worst-case methodology to study the problem of minimizing message delay in the smart grid under jamming attacks:

1. In wireless local-area network Nðm;Nf;NcÞ, for a time-critical application with delay threshold s, what is the worst-case delay performance PðD > sÞ under the generic jamming process ððF; CÞ;XÞ.
2. Given the worst-case scenario in is , how to minimize PðD > sÞ. There has been existing work addressing denial-of-service attacks on multimedia traffic (e.g., [1], [7]). We note that the differences between smart grid traffic and multimedia traffic are: 1) smart grid traffic is more time-critical (e.g., 3 ms requirement in grid compared with around 100 ms requirement for multimedia), 2) time-critical traffic is periodical, unsaturated (i.e., the traffic load smaller than the network bandwidth) in the smart grid, and multimedia traffic is usually saturated and requires adequate congestion control. As a result, the smart grid traffic features a simpler retransmission mechanism

without congestion control. In addition, we will show that we can take advantage of the unsaturated nature of smart grid traffic to design countermeasures. Next, we use theoretical analysis to show the worst-case delay performance under jamming attacks.

3. Theoretical Analysis and Proposed Solution

In this section, we theoretically analyze the worst-case delay performance for wireless smart grid applications under the generic jamming model. We first consider the worst case in coordinated communication, then the worst case in uncoordinated communication. Finally, we propose a method to minimize the worst-case delay for both coordinated and uncoordinated modes.

We have observed that for both coordinated and uncoordinated communications in wireless smart grid applications, the delay performance is sensitive to the network traffic load under jamming attacks. As a result, generating camouflage traffic is promising to improve the worst-case delay performance. In this section, we present our adaptive method that generates camouflage traffic to minimize the message delivery delay in wireless networks for smart grid applications.

3.1 Motivation and System Design

Our goal is to find and design a feasible method to minimize the worst case delay performance for practical wireless smart grid applications under jamming attacks. We first describe the general idea of our method, which can be used for both coordinated and uncoordinated communication optimum. Thus, we design the TACT method (transmitting adaptive camouflage traffic).

The intuition behind TACT is two-fold. 1) TACT should avoid node coordination. Admittedly, node coordination can further help improve the delay performance. However, it introduces an additional security issue of coordination message delivery under jamming. Thus, TACT should be of distributed nature, inducing the minimum complexity and node coordination. 2) Since the worst-case message delay is minimized at a positive traffic load, TACT should always attempt to increase the traffic load. If the performance is degraded after the increase, it can reduce the load.

Accordingly, we propose to implement the TACT method at every node in a wireless network for the smart grid. As shown in Algorithm 1, TACT measures the delivery results of probing messages to adjust the amount of camouflage messages in the network. Each camouflage message is transmitted on a randomly selected frequency/code channel.

Algorithm 1 : TACT at Each Node.

Given: $L, L_{\min}, L_{\max}, \Delta_{\text{inc}}, \Delta_{\text{dec}}$. **Init:** $M_{\text{prev}} = 0, L = L_{\min}$
repeat
  Transmit probing messages in observation period.
  Measure the number of ACKs, M_{now}.
  if Performance not degraded ($M_{\text{now}} \geq M_{\text{prev}}$) **then**
    Increase the traffic load: $L \leftarrow \min(L + \Delta_{\text{inc}}, L_{\max})$.
  else
    Decrease the traffic load: $L \leftarrow \max(L - \Delta_{\text{dec}}, L_{\min})$.
  end if
  Record history: $M_{\text{prev}} \leftarrow M_{\text{now}}$.
until TACT is disabled.

Figure 4 -TACT at every node

3.2 TACT in Coordinated and Uncoordinated Modes

So far, we have presented the fundamentals of TACT to minimize the worst-case message delay under jamming attacks. Although we have shown that uncoordinated 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. Accordingly, we summarize the complete jamming-resilience.

3.3 Objective- To attain Uniform Optimum

When TACT is deployed at node k, it starts to increase node k's traffic load _k. However, increasing _k cannot improve node k's own delay performance since PðDk > sÞ is not a function of _k but a function of gk P m j¼1;j6¼k _j. By transmitting more traffic into the network, node k in fact improves the network traffic loads gi ði 6¼ kÞ observed at other nodes. At the same time, node k is expecting others to do the same to help itself. Thus, the efficiency of TACT relies on such homogenous behavior in all nodes, which however cannot be guaranteed when nodes have evidently heterogenous traffic rates. Consider an extreme case: there are two nodes (nodes 1 and 2) with

routine traffic rates of 1 and 1,000 messages/s, respectively. The optimal loads g1 ¼ g2P ¼ 1,000 under a reactive jammer. Initially, g1 ¼ 2 j¼1;j6¼1 _j ¼ 1;000 and g2 ¼ P 2 j¼1;j6¼2 _j ¼ 1. When TACT starts, node 2 is far from the optimum and keeps increasing its traffic load. In contrast, node 1 immediately reaches the optimum and never generates more traffic to help node 2. Therefore, in order to ensure uniform optimum over all nodes, a solution is to mandate every node have the same minimum traffic load, regardless of their different routine traffic rates. This can be achieved by assigning different minimum camouflage traffic loads Lmin (as given in Algorithm 1) to different nodes. Specifically, let node k's minimum camouflage traffic load LminðkÞ ¼ max1_i_mai _ ak, where ai denotes the (fixed) routine traffic load at node i. Thus, the minimum overall traffic load must be transmitted by every node is uniformly equal to max1_i_mai. In the previous example, we can assign Lmin ¼ 999 and 0 to nodes 1 and 2, respectively. Then, both nodes can have the optimal traffic load when TACT starts. If the optimal load is 1,800 messages/ s, both nodes will increase their camouflage traffic loads until reaching the optimum.

Algorithm 2 : Communication Scheme with TACT.

```
Initialization: Enable TACT.
repeat
  Mode ← Uncoordinated mode.
  Obtain key K and period T_K from gateway.
  Mode ← Coordinated mode.
  Use K for a period of T_K.
until The node leaves the network.
```

Figure 5- Optimum Communication with TACT

In Algorithm 2, all the keys of a node is obtained from the gateway via uncoordinated communication. If two nodes want to communicate with each other, they also need to request the key for such communication from the gateway. Hence, the gateway can be considered as a key management center in the network. It is worthy of note that in Algorithm 2, every node operates on either uncoordinated or coordinated mode. The gateway, however, is required to operate on both modes simultaneously. Unlike IEDs that are embedded computers on power infrastructures, the gateway is usually a computer server equipped with powerful computing and communication abilities [7]; thus, it is reasonable to assume that the gateway is capable of operating on both modes.

4. Experimental Results

When the network is set up, all IEDs first communicate uncoordinatedly with the gateway to obtain their secret keys of channel assignments, then use the keys to communicate in a coordinated manner. As a result, we first consider the uncoordinated case; i.e., we first evaluate how TACT can improve the delay performance of key establishment, and then move on to the coordinated case.

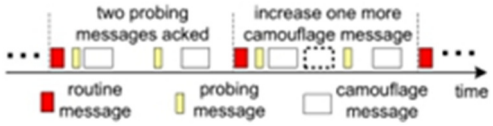

Figure 6- TACT balancing the network traffic.

4.1 Jamming-Resilient Communication

Here, we consider the coordinated mode after the key is established. We evaluate the impact of both reactive and non-reactive jammers on the anti-island application. We generate camouflage messages at rates of 0-30 messages/s. We have seen that reactive jamming always leads to worse performance than non-reactive jamming, indicating that reactive jamming should be considered as the worst-case scenario. Thus, in the following, we will only consider reactive jamming. Fig. 7 also shows that the message invalidation probability induced by reactive jamming is a U-shaped function of the traffic load. We can see that the message invalidation probability decreases from 53.2 percent to 0.657 percent as the camouflage traffic load goes from 0 to 20 messages/s. Then, we consider the delay performance with different delay thresholds of 150, 190, and 230 ms under reactive jamming .If the delay threshold becomes larger, we can transmit the same message more times to ensure more reliability. Thus, the transmissions have five, six, and seven hops (transmission attempts) for messages with delay thresholds of 150, 190, and 230 ms, respectively shows that the message invalidation probabilities for different delay thresholds. In addition, we also compare the worst-case bounds in Theorem 2 with the experimental results, as shown in Fig. 8. Although we can see that that there exists a small and non-uniform gap between the worst-case bound and the experimental measurement for each delay threshold, the performance trends shown by the experimental results do match the theoretical predication and the U-shape phenomena, which indicates that the worst-case bound in Theorem 2 is tight to predict realistic jamming impacts.

Next, we evaluate the effectiveness of TACT against reactive jamming in coordinated communication. Table 1

illustrates message invalidation probabilities in three scenarios: i) frequency hopping under reactive jamming (TACT is off), ii) frequency hopping with camouflage traffic (TACT is on), iii) baseline performance (no jamming, no TACT). It is observed from Table 1 that TACT decreases the message invalidation probability from 53.20 to 0.657 percent. Although TACT does not achieve the minimum probability of 0.235percent shown in Fig.7, it still improves the delay performance in order of magnitude under reactive jamming. Note that the baseline performance in Table 1 show a positive message invalidation probability. This is because error correction is not used in our experiments in order to reduce the GNU Radio processing delay.

Table 2 shows the message invalidation probability as a function of the number of frequency-hopping channels Nf under reactive jamming. It is known that increasing Nf can reduce the message delay for spread spectrum communication, as more spectrum resources are used. Table 3 illustrates that when Nf goes from 5 to 11, the message invalidation probability in the frequency-hopping-only (no TACT) scenario decreases from 91.4 to 11.1 percent; while TACT can further reduce the probability from 11.1 to 0.215 percent. As a result, TACT is a promising mechanism that offers a new dimension to improve the delay performance for smart grid communication systems.

Table1- Message Delay in Coordinated communication.

Set ups	TACT Off	TACT On	Baseline
Delay	53.20%	0.66%	0.05%

Table 2- Message delay probability versus number of frequency channels

No.of channels	5	4	9	11
TACT Off	91.4%	67.2%	40.3%	11.1%
TACT On	14.2%	5.02%	0.724%	0.315%

.

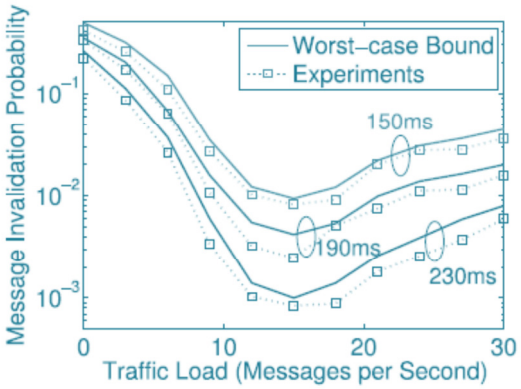

Figure 7- Message invalidation probability with different delay thresholds

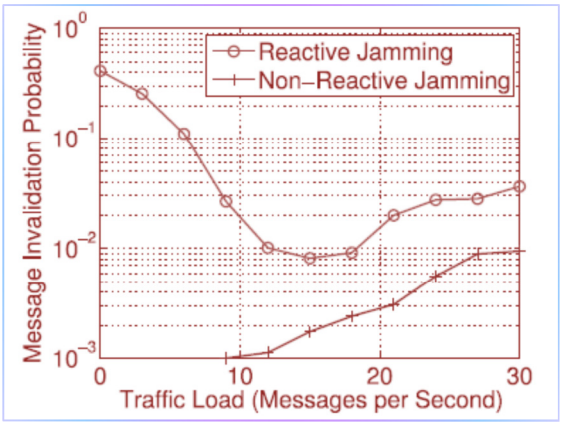

Figure 8-Message invalidation versus traffic load for both type of jamming

5. Conclusion

In this paper, we illustrated a comprehensive study of minimizing message invalidation probability i.e. message delay for the smart grid applications under worst-case jamming attacks. We observed that the worst-case message delay is a U-shaped function of the network traffic load. We proposed a lightweight yet promising method TACT, to generate the camouflage traffic to minimize the message delay for smart grid applications under any potential jamming attack and balance the network load at the optimum point. Both the legitimate and the camouflage traffic are unknown to receivers as well as the attackers, which causes collisions between legitimate and camouflage traffic transmissions. This can be avoided using message concatenation technique which concatenates multiple data into larger packets to reduce protocol overhead and minimize collisions. It hence reduces more delay for smart grid data transmission. The direction of future work suggests how concatenation can be done at the multiple levels of communication networks

in the smart grid and how the legitimate receiver could find the difference between the legitimate and camouflage traffic without exhausting more energy packets. As long as we design our countermeasures based on the worst case, we can always provide performance guarantee under any substantial attack behavior, which is our prime objective and necessity for the smart grid applications.

References

(1) Zhou Lu, Wenye Wang, Clidd Wang, "Camouflage Traffic: Minimizing Mesaage Delay for Samrt Grid Applications under Jamming," IEEE Trans. Dep., vol 12, no.1 , Jan/Feb. 2015

(2) M. Strasser, C. Popper, M. Cagalj: Jamming –resistant Key Establishment using Uncoordinated Frequency Hooping IEEE Symp. Security And Privacy, May 2008.

(3) Randomized Differential DSSS: Jamming Resistant Wireless Broadcast Communication, IEEE Conf. IEEE INFOCOM Mar. 2010

(4) S. Capkun, M. Strasser, C.Popper: Anti-Jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques, IEEE J, vol 28, no.5, June 2010.'

(1) "Smart Grid Cyber Security: Challenges and Solutions" S. Shaphough, R .Aburukba, I. Conf. on smart grid, 2015.

(2) "NetCamo: Camouflaging Network Traffic for QoS-Guaranteed Mission Critical Applications" Y. Gaun, X. Fu, P. Shenoy, R. Bettati, W. Zhao, IEEE Trans. Sys. Cyber, vol 31, no.4, July 2001.

(3) Hiding Traffic with Camouflage: Minimizing Message Delay in the Smart Grid under Jamming, Z. Lou, C. Wang, W. Wang, IEEE Int. Conf. Comput. Comm. 2012.

(4) J. Jiang, Y. Qian: Distributed Communication Architecture for Smart Grid Applications, IEEE Commun. Mag. Dec 0216.

(5) "Camouflage of Network Traffic to Resist Attack (CONTRA)" W. Weinstein, J. Lepanto, IEEE Comput. Society, pro. DARPA 2003.

(6) "A Novel Security Key Recovery Framework for Smart Grid Applications" P. Haudpakanam, C. Pirak, R. Mathar, IEEE APCC 2014.

(7) B. Karimi, V. Namboodiri, M. Jadliwala, "Scalable Meter Data Collection in Smart Grids Through Message Concatenation," IEEE Trans. Smart Grid, vol 6, no. 4, July 2015.

(8) J. Jiang, Y.Qian :Distributed Communication Architecture for Smart Grid Applications, IEEE Communication Magazine, Dec 2016.

(9) "Camouflage of Network Traffic to Resist Attack (CONTRA," W. Wienstein, J. Lepanto, IEEE Computer Society, pro.2003.

(10) "A Novel Security Key Recovery Framework for Smart Grid Applications." P. Haudapaknam, C. Pirak, R. Mathar, IEEE APCC 2014.

(11) B. Karimi, V. Namboodiri, M. Jadliwala: Scalable Meter Data Collection in Smart GridsThrough Message Concatenation, IEEE Trans.on Smart Grid, vol 6, no. 4, July 2015.