A Novel Mechanism for Surveillance Transmission in Smart Grid

Jun Xia[1]; Kai Yu[1†]; Chao Yun[1]; Lingling Li[3]; Haifeng Wang[2]; Zhiyong Bu[1]

[1]*Shanghai Institute of Micro-system and Information Technology , Chinese Academy of Sciences, Shanghai, 200050 China,*

[2]*Renesas Tele. Tech. (Beijing) Ltd., Shanghai Branch, China*

[3]*Institute for China Electronic System Engineering Company, Beijing,, China.*

{jun.xia; kai.yu; zhiyong.bu}@mail.sim.ac.cn; haifeng.wang@renesasmobile.com

***Abstract*—Herein, we propose a novel resilient forwarding mechanism to address the contradictory problem between transmission performance and power saving problems. Through automatic backup and transmission line switch, self-healing and autonomous troubleshooting can be achieved for online monitoring in transmission grid. Autonomous surveillance transmission network can be achieved through transmission line indicators. Even though several parts of the transmission network are breakdown, resilient forwarding mechanism may still provide robust pre-alarming and data transmission services. We also evaluate the performance of our approach by reducing the transmission latency to improve network performance. We further analysis the transmission latency gain with resilient forwarding mechanism through simulations. It is shown that our mechanism outperforms the conventional scheme.**

***Index Terms*-- Resilient forwarding, smart grid, automatic backup, self-healing**

I. INTRODUCTION

Smart grid is a future self-healing power system which is based on the information technology, which will combine the novel control, information and management techniques, realize a series of intelligent interactive activities from power transmission to electricity end users, and scientifically and systematically optimize electricity generation, transmission and distribution. The application of advanced digital technologies (i.e., microprocessor-based measurement and control, communications, computing, and information systems) are expected to greatly improve the reliability, security, interoperability, and efficiency of the electric grid, while reducing the environment impacts and promoting economic growth[1].

In conventional electricity systems, power transmission depends mainly on high voltage electric overhead power lines. The design of overhead power lines can be mainly separated into four individual components: foundations, supports, interfaces and conductors. Note that all of these components have limited mechanical strength [2]. Failure of one or more components will incur the collapse of entire transmission facility. This kind of fragile transmission structure may span a few kilometres, and huge amounts of electrical towers are deployed for mounting long transmission line. These towers take the responsibility for relaying the power transmission line as ordinary supporter. These exposed constructions are often impacted by the nearby environment such as wind, ice, snow, earthquakes,

[†]*Corresponding Author*

flooding, etc. They are also impacted by the human related hazards such as accidents and terrorist activities [3]. Fortunately, most of these negative impacts can be detected and prevented through persistent monitoring and pre-alarm.

Current routine maintenance of electric transmission lines depends mostly on human inspection. With limited inspection methods, once a breakdown happens in certain section of the long transmission line, it is hard to accurately locate the failure point and make prompt troubleshooting. Therefore in smart grid, WSNs are employed for grid status surveillance, including monitoring the physical parameters of electrical tower and the status of the transmission line, such as metal fatigue, wire firmness, etc.

Based on the implementation of WSNs in transmission grid, sensors installed on the towers and electric wires send monitoring data periodically to the local gateway hop by hop. The data required by wide area monitoring and control systems will be provided by smart sensors and sent to the system main controller that is much faster and more accurate than the traditional Supervisory Control and Data Acquisition (SCADA) control systems [4]. Although the power saving problem still makes the practical deployment of WSNs difficult, WSN as a basic awareness part of the communication architecture, is necessary and cannot be replaced in the smart grid. From coverage and connectivity perspective, some long range wireless communication technologies (such as LTE, WLAN, WiMAX) can be used to connect those isolate WSNs. These long range transmission technologies are suitable for the communication backbone in transmission line via multi-hop transmission.

In this paper, we propose a novel conceptual resilient forwarding mechanism to address the contradiction between transmission performance and power saving problems. The rest of this paper is organized as following. Section II introduces some related works and discusses the resilient forwarding mechanism. We present the related works of sensor net in on line monitoring and resilient transmission study in smart grid. Section III proposed an implementation example of chain type forwarding in smart grid with our resilient mechanism. Section IV evaluated the performance of resilient mechanism in chain type network. The conclusion and future work are discussed in Section V.

II. RELATED WORKS

The events that threat the overhead power lines can be categorized into accumulation type and burst type. Accumulation type includes impacts imposed by the environments such as ice, snow, rain, wind, etc. The burst type, on the other hand, includes impacts triggered by natural disaster such as flooding, earthquake, typhoon, etc. Additionally, human hazards like power line theft and terrorist activities are classified as burst type as well. The key difference between accumulation type threat and burst type threat is the reactive time for the transmission grid to respond to the emergency. For instance, ice and snow increase the tensile forces on the wires due to its added weight, which can be pre-alarmed by sensors before the loads on wires overweight. The burst type threat, however, may totally destroy the infrastructure of transmission grid within a short period of time (note that even the sensor deployed in the networks may be destroyed). Noticeably, conventional surveillance methods used in sensor networks can hardly cope with the burst type. WSN as the basic part of the surveillance network in smart grid, need to be further improved to fulfil requirements for smart grid.

It is well known that Yang et al. [5, 6] are the pioneers who have proposed to use sensor networks to monitor overhead transmission lines. Yang et al. further implemented a prototype of the power line sensors to demonstrate its feasibility in [7]. To forward the sensing data back to the substation, wireless communication are one of the most cost-effective approaches in terms of the equipment installation

cost and initial installation time [8]. In transmission line monitoring applications, sensors are usually deployed close to the poles/towers on each span. León et al. proposed to install the accelerometers in the support body for vibration and tilt monitoring, and in the conductor attachment points for detecting wind induced vibration [9]. They also suggested a two layers model to overcome the restrictions imposed by the range/energy management issue on the sensor nodes. Yang et al. suggested the use of ZigBee Pro in an open area [8]. But the communications range of sensors is limited by the power supply [10–12]. However, the achievable transmission range can still allow a relay node to communicate with its two nearby relay nodes, which is similar to the concept proposed by León. These devices installed on the towers are so-called transmission gateways equipped with both WSN module and long range wireless module.

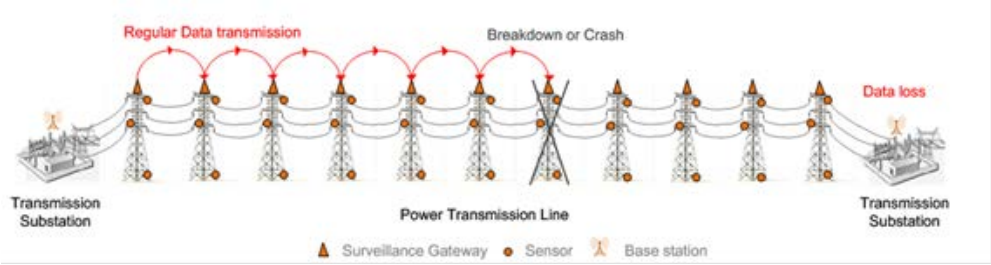

Fig.1 Failure of transmission line caused by intermediate gateway breakdown

In general, transmission procedure between gateways behaves in a periodic manner. Two separate substations are linked by several electrical towers scattered in tens of kilometers or even hundreds of kilometers. Sensor nodes deployed on the towers send surveillance data to the gateway located on the top via local solo tower sensor network. Gateways on each tower incorporate the packages and participate in the regular data transmission procedure. Finally, the receiving substation receives the monitoring data through multi-hop relaying.

However, burst type threat may occasionally cause the breakdown of certain gateways. Since the surveillance reporting link based on gateways installed on transmission tower is one-way link, intermediate gateway breakdown will trigger cascading malfunction and finally cause the failure of the whole surveillance line data transmission. This worst-case situation is shown in Fig.1, as the gateway on intermediate tower breaks down, the remaining communication links to the substation will be lost subsequently. Obviously, any intermediate gateway crash may paralyze the whole reporting network; therefore this network topology is not robust.

III. RESILIENT FORWARDING MECHANISM

To overcome the weakness of chain type transmission and enhance the robustness of transmission surveillance procedure, we propose a resilient forwarding mechanism in smart grid. The mechanism overcomes the drawback of chain reporting pattern. Once certain gateway initiates the forwarding process, it sends the sensory data to adjacent gateways via a broadcasting manner. The adjacent gateway with different line number (which will be explained later), so-called backup gateway, receives the message from previous gateway.

The backup gateways only backup the message rather than forwarding the message immediately. Afterwards, during the forwarding process, if the backup gateway does not detect the data transmission activity of its next gateway in predefined time slot, backup gateway can forward the data stored in its local storage to the next hop gateway with same line number. This is because the backup gateway knows that certain gateway on the relay line does not work properly. For the mechanism to operate

properly, each gateway possesses an indicator consisted of three parts: original line number, current line number and suspending flag. Gateway can switch between different transmission lines according to the indicator in the received packet.

Assuming a homogeneous gateway is deployed on each transmission tower. During the surveillance network data exchange phase, each gateway communicates in a TDM fashion. All data exchanging process have to be restricted in the time slot predefined in the network initialization stage. Each gateway can switch its own status according to the condition of its adjacent gateways.

Transmission gateways installed on electrical transmission towers are divided into groups. Each transmission tower is assigned a unique identification in transmission line. For instance, the first number refers to group index and the second number refers to current tower ranking in group comprise an integrated identification. As depicted in Fig.3, there are four transmission groups in transmission line with number 1~4. Three member towers are allocated in each transmission group, which are allocated number 0~2 to indicate the line number. For example, tower #20 belongs to group #2 and also belongs to line #0. Towers #10, #20, #30, #40 all comprise transmission line #0.

In Fig.2, periodic equipment examination process is initiated by the transmission substation. In a routine examination, towers with the same line number in different groups form an independent transmission line in a multi-hop fashion. In this case, there are three transmission lines: line #0, line #1 and line #2. Once line #0 switches into operating pattern, the other two lines are in the backup mode.

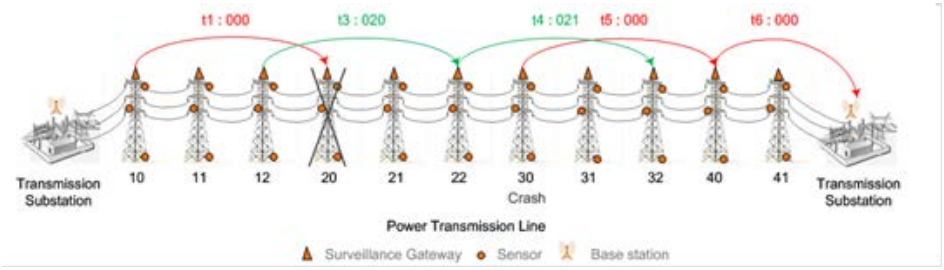

Fig.2 The original line breakdown scenario

For instance, at the very beginning, tower #10 initiates a data report process and transmit surveillance sensory data to tower #20. Unfortunately, tower #20 breaks down at this moment. Surveillance data cannot be relayed and forwarded to tower #30. However, tower #11 and tower #12 have recorded the sensory data from tower #10 during its transmission period since tower #10 operated in broadcasting fashion. Tower #12 keeps listening in the adjacent transmission slots to confirm whether tower #20 starts the forwarding process. If tower #12 didn't probe any transmission activity of tower #20, it indicates the forwarding process at tower #20 is failed. Then tower #12 starts backup transmission process by broadcasting data cached previously in local storage during the following time slot. Meanwhile, tower #11 keeps waiting for the transmission activity of tower #12 and ready for backup transmission. Once tower #12 starts the backup process, tower #11 can probe the activity of tower #12 and switch into power saving mode.

Similarly, this backup transmission use line #2 via the same process of line #0. But as the sensory data on the following towers with line number #0 (such as tower #30 and tower #40) are also necessary for data collection, transmission line needs to switch from line #2 back into the line #0. Through the line switching process, the tower that breaks down can be bypassed. Here, the indicator is attached on each transmission as described in Fig.3. For example, during the line #0 operation period in t1, the indicator is set as 000. After the backup process started, the indicator is set as 020 in t3. The 2nd digit of the indicator indicates the current workable line is line #2 and 1st digit reveals the original line is

line #0. The 3rd digit, suspending indicator here is used for bypassing the tower at fault. As the suspending indicator is set to 0, current relay tower can forward data packets immediately.

If original line and current line number in the indicator are not the same, we can draw a conclusion that the current transmission is operating on the backup line. Once the transmission line has been switched into backup line, transmission tower on backup line set the suspending indicator to 1. If forwarding gateways on the backup line detect the positive suspending indicator, it will wait for one transmission slot after received data from the prior gateway. During such time slot, if the backup gateway detects gateway transmission activity of gateway on original line, forwarding process via backup line will be terminated until next transmission slot. According to this, the transmission line will be switched to the original line. Such process is depicted in Fig.3, while tower #32 waits one slot to transmit and keep listening for the activity of tower #30. Afterwards, tower #32 terminates its forwarding process since tower #30 switches into active mode.

In terms of the tower #30, it received the sensory data from tower #22 and checks the indicator. Since the indicator is 021, which shows the current transmission line is the backup line for line #0 and tower #30 has to take responsibility to forwarding the data rather than other gateways on the backup line. Thus tower #30 starts forwarding process instantaneously. Meanwhile the backup forwarding process is terminated autonomously.

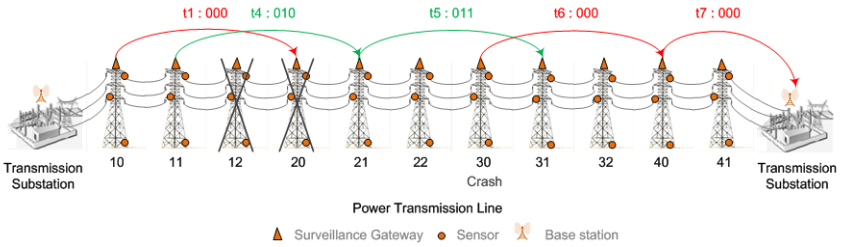

Fig.4 Successive gateways breakdown scenario

Since the gateway are homogeneous, gateway on backup line may also have certain possibility be out of order. As illustrated in Fig.4, tower #12 breaks down as tower #20. Crash of tower #12 will certainly cause the backup line switching failure in line #2. However, in this resilient forwarding mechanism, switching between each backup line can also be achieved spontaneously and efficiently. Since gateway #11 has not probed the transmission activity of gateway #20 during its duty slot, tower #11 considers the switching process in line #2 failed, and starts the backup forwarding in backup line #1.

In the backup line switching procedure, work slot distribution of each tower needs to be further clarified. In the network pre-implementation period, each gateway's work slot and sequence number in group are pre-defined. In periodic transmission line maintenance process, each transmission line start reporting surveillance sensory data in order. We assume the gateway can communicate with several adjacent towers within its transmission range. To make it clear, we combine the activation and forwarding process in a single time slot, since the activation is not our main focus.

IV. PERFORMANCE EVALUATION

To simplify our analysis, the following assumptions are made here: There are N towers in a section between two facilities connected to the internet (e.g. substation or tower with internet connection). However, these N towers can not connect directly to the internet themselves. The data transmission rate of gateway equipped with long range wireless transmission devices is R bps. The

entire gateways installed on the towers transmit sensory data using the same data rate. Total data size per gateway in each transmission round is set as D bits. Parameter α denotes the path loss factor in a surveillance wireless transmission scenario. There are n_g towers implemented in each resilient transmission group, which also means there are n_g transmission lines in resilient surveillance system. Data exchange process transmits on the time slot predefined in the surveillance network initialization stage, no collision happens during transmission period.

Based on the above assumptions, we first analyze the time delay in conventional hop by hop transmission scenario. In the routine maintenance manner, each gateway needs to report its local sensor data via relay nodes. Once an intermediate gateway receives sensory data from its nearby gateways, it will send its data together with the precious data. Thus the transmission delay of the chain topology network in conventional procedure can be calculated as:

$$Latency_{conv} = \frac{DN(N+1)}{2R} \tag{1}$$

From equation (1), it is easy to find that the transmission delay in chain topology network is mainly decided by the square of N in chain network. Similarly, we can analyze the delay in chain topology network with resilient mechanism:

$$Latency_{res} = n_g \times \frac{D\frac{N}{n_g}\left(\frac{N}{n_g}+1\right)}{2R} = \frac{DN(N+n_g)}{2Rn_g} \tag{2}$$

Since in the resilient forwarding procedure, different transmission lines have to start data exchanging in an orderly fashion. We compare the latency in conventional case and the latency in resilient forwarding case below.

$$Latency_{gain} = Latency_{conv} - Latency_{res} = \frac{DN^2(n_g-1)}{2Rn_g} \tag{3}$$

From equation (3), we can discover that the gain of latency is achieved by resilient forwarding mechanism while n_g is set properly. With the increase of n_g, which means higher number of towers in each group, we can achieve more latency gain in practical deployment. With resilient forwarding mechanism, higher latency gain can be obtained through low transmission rate as shown in Fig.3, which is similar to the current engineering situation.

Note that in practical situation (especially in an urgent case), the intermediate gateway may notice some special events are happening based on local sensor data. A pre-alarming procedure may trigger immediately and a warning message is sent to the substation as soon as possible. In this case, with resilient forwarding mechanism, warning message can reach the substation with fewer hops and latency.

In practical network, when the scale of the network grows (the number of towers in the transmission chain increases), the tower close to the destination needs to forward more data to the destination. However, resilient forwarding method can release such transmission bottleneck via dividing towers into different transmission groups. As shown in Fig.4, more latency gain can be achieved in a larger network with more towers. With the same transmission rate, smaller data size can bring more transmission efficiency benefits.

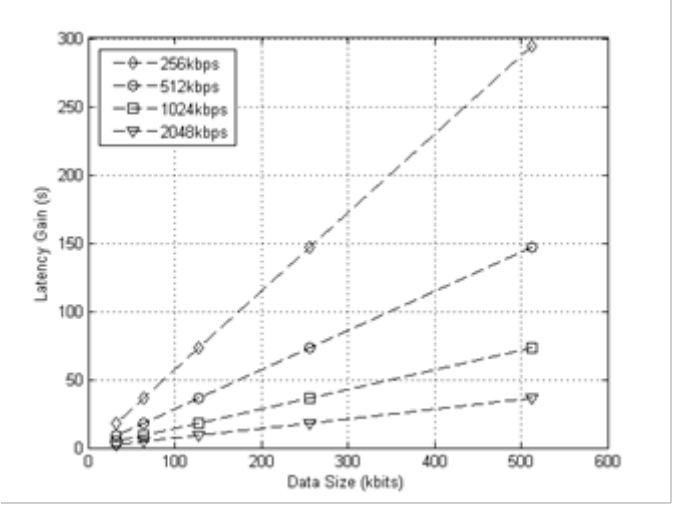

Fig.3 Latency Gain v.s. data size

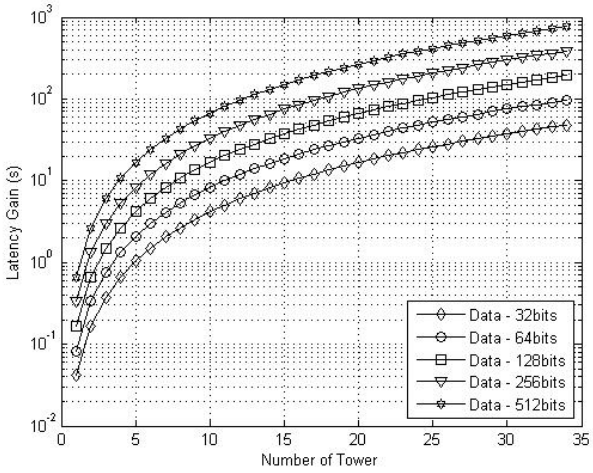

Fig.4 Latency Gain v.s. number of towers

Noticeably, as part of self-healing technology in smart grid, resilient transmission mechanism can mitigate and prevent the negative impacts caused by natural disasters and human hazards. As pointed out in a report published by State Grid Corp. of China [10], the real-time surveillance, as well as pre-alarming mechanism of high-voltage transmission backbone is two important goals of smart grid construction. Since the density of transmission grid deployment is pretty high in China, resilient transmission scheme will play an important role in the future smart grid.

V. CONCLUSION

In this paper, a resilient forwarding mechanism has been proposed to relieve the fragile network topology problem and enhance the flexible of surveillance sensory data transmission. In this resilient forwarding mechanism, transmission efficiency can be enhanced by saving unnecessary handshaking signalling. Therefore the infrastructure deployment cost can be lowered for realistic deployment. Monte-Carlo simulations have been used to show the performance gain of using our novel resilient forwarding mechanism

ACKNOWLEDGEMENT

This paper is conducted within Tri-lateral Renesas-SIMIT-SGETRI Smart Grid Standard Research Collaboration Project, and is partly supported by Renesas Mobile Corporation.

REFERENCES

[1] Report to NIST on the Smart Grid Interoperability Standards Roadmap, www.nist.gov/smartgrid/upload/Report_to_NIST_August10_2.pdf

[2] F. Kiessling, P. Nefzger, J. F. Nolasco, and U. Kaintzyk, Overhead Power Lines – Planning, Design, Construction. Berlin, Germany:Springer-Verlag, 2003.

[3] R. A. Leon, V. Vittal, G. Manimaran, "Application of sensor network of secure electric energy infrastructure," IEEE Transactions on Power Delivery, vol. 22, no. 2, April 2007.

[4] Cecati. C, Mokryani. G, Piccolo. A, Siano. P, "An overview on the smart grid concept," IECON 2010 - 36th Annual Conference on IEEE Industrial Electronics Society , vol., no., pp.3322-3327, 7-10 Nov. 2010

[5] Y. Yang, D. Divan, R. G. Harley, and T. G. Habetler, "Power line sensornet - a new concept for power grid monitoring," in IEEE Power Engineering Society General Meeting, 2006.

[6] Y. Yang, F. Lambert, and D. Divan, "A survey on technologies for implementing sensor networks for power delivery systems," in IEEE Power Engineering Society General Meeting, 2007.

[7] Y. Yang, D. Divan, R. G. Harley, and T. G. Habetler, "Design and implementation of power line sensornet for overhead transmission lines," in IEEE Power Engineering Society General Meeting, September 2009.

[8] V. C. Gungor , F. C. Lambert, "A survey on communication networks for electric system automation," Computer Networks, vol. 50, pp. 877–897, 2006.

[9] R. A. Leon, V. Vittal, G. Manimaran, "Application of sensor network of secure electric energy infrastructure," IEEE Transactions on Power Delivery, vol. 22, no. 2, April 2007.

[10] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp.102–114, Aug. 2002.

[11] D. Culler,D. Estrin, and M. Srivastava, "Overview of sensor networks," IEEE Computer., vol. 37, no. 8, pp. 41–49, Aug. 2004.

[12] F. L. Lewis, "Wireless sensor networks," in Smart Environments: Technologies, Protocols, and Applications,D. J. Cook and S. K. Das, Eds. New York: Wiley, 2004.